群　論

近藤　武著

岩波基礎数学選書

岩波書店

群　論

監　修
小　平　邦　彦

編　集
岩　堀　長　慶
河　田　敬　義
藤　田　　　宏
小 松 彦 三 郎
田　村　一　郎
服　部　晶　夫
飯　高　　　茂

群　　論

近藤　武著

岩波基礎数学選書

岩　波　書　店

刊行にあたって

——数学的現象の把握を——

現代の数学は形式主義の影響を強くうけていて，数学の本にも，定義，公理，定理，証明を羅列した形式で書かれたものが多い．形式主義によれば，数学はそれ自身は意味をもたない記号を与えられたルールに従って並べて行くゲームに過ぎないということであるが，これは数学の最も本質的なものを見落しているのではなかろうか？　たとえば，公理的構成の規範となったHilbertの幾何学基礎論では，'点'，'直線'，等は意味のない無定義語，すなわち記号であって，'猫'，'雀'，等で置き換えても一向差支えないことになっているが，これは事実に反する．実際，Hadamardが指摘したように，幾何学基礎論には殆んど毎頁に図が載っている．図を描かず，頭の中で図を想像することもせずに，論理だけによってHilbertの幾何学基礎論を理解することは不可能であろう．このように 意味を考えない形式主義の立場に立つ限り，幾何学基礎論さえも理解できないのである．

私の見る所では，数学は実在する数学的現象を記述しているのであって，数学を理解するということは，窮極において，その記述する数学的現象のイメージを言わば感覚的に把握し，形式主義では捕捉できない数学の意味を理解することである．

岩波講座「基礎数学」は現代の数学の基礎部門の基本的な内容を上述の意味で感覚的にわかり易く解説することを目標として編集された．このたびのシリーズはこの講座の中から学部程度の基礎教科に相当するものを選び「岩波基礎数学選書」として編集しなおしたものである．

この機会に章末問題に対して解答・ヒントを付し，学生の勉学に供するようにした．

1990年6月

小 平 邦 彦

目　　次

第1章　群の概念

この章では群の定義と群を取り扱う上に必要な諸概念——部分群，剰余群，準同型，生成系，共役類——について説明する．同時に群のいろいろな実例——線型群，対称群，正多面体群，正2面体群など——を与える．最後の§1.7では群とともに代数学の基本概念である環と体について説明し，それに関連した群論的事項について述べる．

§1.1　群の概念

a）半　群

Sを任意の集合とする．直積集合$S\times S$からSへの或る写像fが指定されているとき，Sの上に演算が定義されているという：

$$S\times S\ni(x,y)\longmapsto f(x,y)\in S.$$

いいかえると，Sの2元の順序づけられた任意の組(x,y)に対してSの第3の元$f(x,y)$を定める規則が与えられているとき，Sの上に演算が定義されているというのである．

本書では演算を乗法で表わすことが多い．すなわち写像の記号$f(x,y)$を用いずに，$f(x,y)$を単にxyと書くのである．xyをxとyを結合して得られる元ということがある．$S\ni x,y,z$のとき，xyとzを結合して得られる元を$(xy)z$，xとyzを結合した元を$x(yz)$と書く．

結合法則　Sの元x,y,zに対して，つねに

$$(xy)z=x(yz)$$

が成り立つとき，この演算は結合法則を満たすといい，Sは(この演算に関して)**半群**であるという．

半群Sのn個の元の列

$$x_1,\ x_2,\ \cdots,\ x_n$$

に対し，となり合った2元x_{i-1},x_iを結合して$n-1$個の元の列

$$x_1,\ \cdots,\ x_{i-2},\ x_{i-1}x_i,\ x_{i+1},\ \cdots,\ x_n$$

を作り，さらにこの列のとなり合った或る2元を結合して $n-2$ 個の元の列を作る．明らかにこの操作を $n-1$ 回続ければ，S の元が定まる．たとえば $n=4$ とすると，結合の順序を括弧で示すことにすれば，

$$((x_1x_2)x_3)x_4,\quad (x_1(x_2x_3))x_4,\quad x_1((x_2x_3)x_4),\quad x_1(x_2(x_3x_4)),\quad (x_1x_2)(x_3x_4)$$

なる見掛け上5個の S の元が得られるが，これらの元は結合法則を繰返し用いればすべて等しいことが容易に確かめられる．一般につぎの法則が成り立つ：

一般結合法則　$S\ni x_1, x_2, \cdots, x_n$ $(n\geqq 3)$ のとなり合った2元をつぎつぎに結合して S の元を作るとき，結合の仕方によらずに S の同一の元が定まる．

[証明]　$n=3$ のときは結合法則にほかならない．$x_1, x_2, \cdots, x_n$ をこの順序に従って順番に結合して得られる元を $x_1x_2\cdots x_n$ と書く：たとえば $((x_1x_2)x_3)x_4 = x_1x_2x_3x_4$．以下 $S\ni x_1, x_2, \cdots, x_n$ $(n\geqq 3)$ が与えられたとき，となり合った2元を結合していく仕方によらず最終的に得られる元が $x_1x_2\cdots x_n$ に等しいことを n に関する数学的帰納法によって示そう．まず最初に x_{i-1} と x_i を結合したとする．このとき $n-1$ 個の元の列

$$x_1,\ \cdots,\ x_{i-2},\ x_{i-1}x_i,\ x_{i+1},\ \cdots,\ x_n$$

が得られるが，数学的帰納法の仮定によりこれからあとは結合の仕方の如何を問わず最終的に得られる元は

$$(*)\qquad x_1x_2\cdots x_{i-2}(x_{i-1}x_i)x_{i+1}\cdots x_n$$

に等しい．ところで結合法則により

$$x_1x_2\cdots x_{i-2}(x_{i-1}x_i) = (x_1x_2\cdots x_{i-1})x_i$$

であるから(*)は $x_1x_2x_3\cdots x_n$ に等しいことがわかる．▌

半群 S の元 e が

$$(1.1)\qquad xe = ex = x \qquad (\forall x\in S)$$

を満たすとき，e を S の**単位元**という．半群が単位元 e をもてば，e は一意的に定まる．実際 e, e' がともに(1.1)を満たせば

$$e' = ee' = e$$

である．ここで第1の等号は e が(1.1)を満たすことから得られ，第2の等号は e' が(1.1)を満たすことから得られる．単位元はしばしば1で表わされる．このときには数字の1と混同しないように注意すべきである．

単位元1をもった半群 S の元 x に対して

$$xx' = x'x = 1 \tag{1.2}$$

を満たす x' が存在するとき，x' を x の**逆元**という．$S \ni x$ が逆元をもつとき，その逆元は一意的である．実際 x', x'' がともに(1.2)を満たせば

$$x' = x'1 = x'(xx'') = (x'x)x'' = 1x'' = x''$$

となる．x の逆元は x^{-1} で表わされる．

問 1.1 $1^{-1}=1$ である．また x, y がともに逆元をもてば，$(x^{-1})^{-1}=x$，$(xy)^{-1}=y^{-1}x^{-1}$．——

S における演算を加法で表わすこともある：

$$S\times S \ni (x, y) \longmapsto x+y \in S.$$

このときには，結合法則は

$$(x+y)+z = x+(y+z) \qquad (\forall x, y, z \in S)$$

となる．演算が加法で表わされている半群が単位元をもつとき，それは通常 0 で表わされる．すなわち 0 は

$$x+0 = 0+x = x \qquad (\forall x \in S)$$

なる性質をもつ S の元である．また $S \ni x$ が逆元をもつとき，それは $-x$ で表わされる：

$$x+(-x) = (-x)+x = 0.$$

なお演算を加法で表わすのは

交換法則 $\qquad x+y = y+x \qquad (\forall x, y \in S)$

が成り立つとき用いるのが普通である．

b) 群の定義

集合 G の上に演算

$$G\times G \ni (x, y) \longmapsto xy \in G$$

が定義されていて

I　G は(この演算に関して)半群である，

II　G は単位元をもつ，

III　G の各元は逆元をもつ，

なる三つの公理が満たされているとき，G を**群**という．念のため I，II，III を具体的に書けば，

I　$(xy)z = x(yz) \quad (\forall x, y, z \in G)$，

Ⅱ　$G \ni \exists 1,\quad x1 = 1x = x\ (\forall x \in G)$,

Ⅲ　$G \ni \forall x,\quad G \ni \exists x^{-1},\quad xx^{-1} = x^{-1}x = 1$

となる．群 G が有限個の元からなるとき，G を**有限群**，G の元の数を G の**位数**という．

a) で注意したように群 G において単位元はただ一つ存在し，G の各元 x に対しその逆元 x^{-1} もただ一つ定まる．また公理Ⅰ,Ⅱ,Ⅲからわかるつぎのことは基本的である：

(1.3)　$G \ni a$ を固定する．このとき G から G への写像

$$x \longmapsto ax \qquad (x \in G)$$

は全単射である．すなわち G の任意の元 b に対し $ax=b$ を満たす x はただ一つ存在し，$x=a^{-1}b$ である．実際,

$$ax = b \Longrightarrow a^{-1}(ax) = a^{-1}b \Longrightarrow (a^{-1}a)x = a^{-1}b$$
$$\Longrightarrow 1x = a^{-1}b \Longrightarrow x = a^{-1}b.$$

逆に $x=a^{-1}b$ は，$ax=b$ を満たす：$a(a^{-1}b)=(aa^{-1})b=1b=b$．同様に，

(1.3)′　G から G への写像

$$x \longmapsto xa \qquad (x \in G)$$

は全単射である．すなわち G の任意の元 b に対し，$xa=b$ を満たす x はただ一つ存在し，$x=ba^{-1}$ である．

問 1.2　G から G への写像 $x \mapsto x^{-1}$ は全単射である．

注意　(1.3) から "$ax=a \Longrightarrow x=1$" である．したがって，群の公理Ⅱによれば G の元 e が単位元であるためには，**すべての** a に対して "$ae=ea=a$" であることが要請されているのに対し，実際には**或る元** a に対し $ae=a$ であれば e は単位元である．また (1.3) から "$aa'=1 \Longrightarrow a'=a^{-1}$" であるから，群においては，$aa'=1$ のとき，$a'a=1$ は自動的に成り立つ．

問 1.3　群の公理をつぎのように弱めてもよいことを示せ．

Ⅰ′　$(xy)z = x(yz)\quad (\forall x, y, z \in G)$,

Ⅱ′　$G \ni \exists 1,\quad x1 = x\ (\forall x \in G)$,

Ⅲ′　$G \ni \forall x,\quad G \ni \exists x^{-1},\quad xx^{-1} = 1$. ——

群 G の空でない部分集合 H が

(α)　$H \ni x, y \Longrightarrow xy \in H$,

(β) $H \ni x \Longrightarrow x^{-1} \in H$

を満たすとき，H を G の**部分群**という．(α), (β) から，H は G と同じ演算で群になることがわかる．定義からわかるようにいくつかの部分群(無限個でもよい)の共通部分は部分群である．

問 1.4 群 G の空でない部分集合 H が

$$H \ni x, y \Longrightarrow x^{-1}y \in H$$

なる条件を満たせば，H は部分群である．——

G 自身や単位元のみからなる部分集合 $\{1\}$ は G の部分群である．これらの部分群は，**自明な部分群**とよばれる．G 自身と異なる部分群を G の**真の部分群**，単位元のみからなる部分群を**単位群**という．

群のもっとも基本的な例について述べよう．

例 1.1 線型群 複素数を成分とする n 次正方行列の集合を $M_n(\boldsymbol{C})$ とする．行列の積は結合法則を満たすから $M_n(\boldsymbol{C})$ は行列の積に関して半群である．

$$GL_n(\boldsymbol{C}) = \{A \in M_n(\boldsymbol{C}) \mid \det A \neq 0\} \qquad (\det A \text{ は } A \text{ の行列式})$$

とおけば，$GL_n(\boldsymbol{C}) \ni A, B$ ならば $GL_n(\boldsymbol{C}) \ni AB$ だから，$GL_n(\boldsymbol{C})$ の上に演算が定義されている．このとき，$GL_n(\boldsymbol{C})$ はこの演算に関して群となる．実際，行列の積は結合法則を満たし，単位行列

$$E_n = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

が $GL_n(\boldsymbol{C})$ の単位元であり，$GL_n(\boldsymbol{C}) \ni A$ の逆行列 A^{-1} が A の逆元である．

$$SL_n(\boldsymbol{C}) = \{A \in GL_n(\boldsymbol{C}) \mid \det A = 1\}$$

とおくと，$SL_n(\boldsymbol{C})$ は $GL_n(\boldsymbol{C})$ の部分群である．実際

$$SL_n(\boldsymbol{C}) \ni A, B \Longrightarrow \det AB = \det A \det B = 1 \Longrightarrow AB \in SL_n(\boldsymbol{C}),$$
$$SL_n(\boldsymbol{C}) \ni A \Longrightarrow \det A^{-1} = (\det A)^{-1} = 1 \Longrightarrow A^{-1} \in SL_n(\boldsymbol{C})$$

であるから，部分群であるための条件 (α), (β) が満たされる．$GL_n(\boldsymbol{C})$ を複素数体 $\boldsymbol{C}$ 上の **n 次一般線型群**，$SL_n(\boldsymbol{C})$ を $\boldsymbol{C}$ 上の **n 次特殊線型群**という．n 次ユニタリ行列の集合

$$U(n) = \{A \in GL_n(\boldsymbol{C}) \mid A^*A = AA^* = E_n\} \qquad (A^* = {}^t\overline{A})$$

も $GL_n(\boldsymbol{C})$ の部分群である．これを **n 次ユニタリ群**という．

$$SU(n) = SL_n(\boldsymbol{C}) \cap U(n) = \{A \in U(n) \mid \det A = 1\}$$

とおけば，これも $GL_n(\boldsymbol{C})$ の部分群である．これを **n 次特殊ユニタリ群**という．これらに対応して行列の成分を実数に限ることにより，実数体 $\boldsymbol{R}$ 上の n 次一般線型群 $GL_n(\boldsymbol{R})$，$\boldsymbol{R}$ 上の n 次特殊線型群 $SL_n(\boldsymbol{R})$ が定義される．またユニタリ群に対応して実直交行列の集合

$$O(n) = \{A \in GL_n(\boldsymbol{R}) \mid {}^tAA = A{}^tA = E_n\}$$

は，$GL_n(\boldsymbol{R})$ の部分群である．これを **n 次（実）直交群**という．また $SO(n) = SL_n(\boldsymbol{R}) \cap O(n)$ を **n 次特殊（実）直交群**という．なお，§1.7 で述べるように，任意の体の上の一般線型群，特殊線型群が同じように定義される．

例 1.2　対称群と交代群　Ω を任意の集合とする．Ω から Ω へのすべての写像の集合 $\mathfrak{M}(\Omega)$ は写像の積に関して半群である．すなわち $\mathfrak{M}(\Omega) \ni f, g$ に対して

$$fg(x) = f(g(x)) \qquad (x \in \Omega) \tag{1.4}$$

によって積 fg を定義するとこの演算は結合法則を満たす．さて Ω から Ω への全単射の集合を $\mathfrak{S}(\Omega)$ としよう．$\mathfrak{S}(\Omega) \ni f, g$ ならば $\mathfrak{S}(\Omega) \ni fg$ だから，$\mathfrak{S}(\Omega)$ の上に演算が定義されている．このとき $\mathfrak{S}(\Omega)$ はこの演算に関して群となる．実際，この演算は結合法則を満たし，恒等写像（Ω の各元に自分自身を対応させる写像）が $\mathfrak{S}(\Omega)$ の単位元であり，$\mathfrak{S}(\Omega) \ni f$ の逆写像 f^{-1} が f の逆元である．

注意　上では写像の積を (1.4) のように定義したが，ときには $\mathfrak{M}(\Omega) \ni f, g$ の積を

$$fg(x) = g(f(x)) \qquad (x \in \Omega) \tag{1.4$'$}$$

のように定義することもある．このように写像の積を定義するときには，x の f による像を $f(x)$ で表わすよりは

$$x^f \quad \text{あるいは} \quad xf$$

のように書く方が便利である．この記法を用いるとき (1.4)′ は，

$$x^{fg} = (x^f)^g \quad \text{あるいは} \quad x(fg) = (xf)g \tag{1.4$''$}$$

となる．本書ではとくに断わらないときには，写像の積の定義は (1.4) に従うが，便宜上 (1.4)″ も用いるであろう．なお，積のどちらの定義を用いても，$\mathfrak{S}(\Omega)$ の群としての構造は同じである（§1.3 問 1.24 参照）．

例 1.2 に戻って，Ω が n 個の元からなる有限集合のとき $\mathfrak{S}(\Omega)$ を **n 次対称群**といい，ときには簡単に $\mathfrak{S}_n$ で表わす．$\mathfrak{S}_n$ は $n!$ 個の元からなるから，位数 $n!$ の有限群である．n 次対称群の元を n 次の**置換**という．置換については行列式

の定義に用いられる程度のことは既知とするが，一応簡単なことを復習しておこう．簡単のため $\Omega=\{1,2,\cdots,n\}$ とする．$\mathfrak{S}(\Omega)=\mathfrak{S}_n$ の元 σ は

$$\sigma(1)=i_1,\quad \sigma(2)=i_2,\quad \cdots,\quad \sigma(n)=i_n$$

のとき，

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}$$

で表わされる．$\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$, $\tau=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ の積は (1.4) により

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

となる．(もし写像の積が (1.4)′ のように定義されていれば $\sigma\tau=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$ となることに注意.) σ が p 個の文字 $i_1, i_2, \cdots, i_p$ $(2\leqq p\leqq n)$ を，

$$\sigma(i_1)=i_2,\quad \sigma(i_2)=i_3,\quad \cdots,\quad \sigma(i_{p-1})=i_p,\quad \sigma(i_p)=i_1$$

のように巡回的に移し，その他の文字を不変にするとき σ は長さ p の**巡回置換**とよばれ，$\sigma=(i_1\ i_2\ \cdots\ i_p)$ で表わされる．たとえば

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}=(1\ 2\ 3\ 4),\qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}=(1\ 2\ 3)$$

である．とくに長さ 2 の巡回置換を**互換**という．つぎのことが知られている：

(1.5) 任意の置換は共通の文字を含まない巡回置換の積として書き表わされる．この表示は巡回置換の積の順序を無視して一意的である．

たとえば

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}=(1\ 2)(3\ 4)=(3\ 4)(1\ 2),$$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 6 & 3 & 5 & 1 & 2\end{pmatrix}=(1\ 4\ 5)(2\ 6)=(2\ 6)(1\ 4\ 5)$$

である．

(1.6) 任意の置換は互換の積として書き表わされる．このとき偶数個の互換の積として書けるか奇数個の互換の積として書けるかは与えられた置換によって定まる．偶数個の互換の積として書き表わせるものを**偶置換**，奇数個の互換の積として書き表わせるものを**奇置換**という．

たとえば

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} = (1\ 2)(3\ 4) \quad \text{は偶置換,}$$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 6 & 3 & 5 & 1 & 2\end{pmatrix} = (2\ 6)(1\ 5)(1\ 4) \quad \text{は奇置換}$$

である. $\mathfrak{S}_n \ni \sigma$ に対し

$$\text{(1.7)} \qquad \operatorname{sgn}(\sigma) = \begin{cases} +1 & (\sigma \text{ が偶置換のとき}), \\ -1 & (\sigma \text{ が奇置換のとき}) \end{cases}$$

とおき, これを置換 σ の**符号**という. $\mathfrak{S}_n$ のすべての偶置換の集合は $\mathfrak{S}_n$ の部分群である. これを **n 次交代群**といい, $\mathfrak{A}_n$ で表わす. $\mathfrak{A}_n$ は位数 $n!/2$ の有限群である.

問 1.5 $\mathfrak{S}_3, \mathfrak{S}_4$ の各元を共通の文字を含まない巡回置換の積, 互換の積として書き表わせ. ——

群 G が公理 I, II, III のほかに

IV **交換法則** $\qquad xy = yx \qquad (\forall x, y \in G)$

を満たすとき, G を**可換群**あるいは **Abel 群**という. たとえば0でない複素数の集合 $\boldsymbol{C}^*$ は, 複素数の乗法に関して群であるが(これは例1.1における $GL_1(\boldsymbol{C})$ にほかならない), 明らかにIVを満たすから Abel 群である. Abel 群における演算はしばしば加法で表わされる:

$$G \times G \ni (x, y) \longmapsto x+y \in G.$$

a) でも述べたように演算が加法で表わされた Abel 群においては, 単位元は0で表わされ**零元**とよばれる. また $G \ni x$ の逆元は $-x$ で表わされる. 念のため Abel 群の公理を加法で書けば,

I $\quad (x+y)+z = x+(y+z) \quad (\forall x, y, z \in G)$,

II $\quad G \ni \exists 0, \quad x+0 = 0+x = x \ (\forall x \in G)$,

III $\quad G \ni \forall x, \quad G \ni \exists -x, \quad x+(-x) = (-x)+x = 0$,

IV $\quad x+y = y+x \quad (\forall x, y \in G)$

となる. 演算が加法で書かれた Abel 群を**加法群**あるいは**加群**とよぶこともある.

例 1.3 $\boldsymbol{Z}^n$ を成分が整数の n 項(行)ベクトル

$$x = (x_1, x_2, \cdots, x_n) \qquad (x_i \in \boldsymbol{Z})$$

の全体の集合とすると，数ベクトルの加法に関して $\boldsymbol{Z}^n$ は加法群となる．零元は

$$0=(\underbrace{0,0,\cdots,0}_{n})$$

であり，$x=(x_1,x_2,\cdots,x_n)$ の逆元は

$$-x=(-x_1,-x_2,\cdots,-x_n)$$

である．同様に複素数を成分とする n 項(行)ベクトルの集合 $\boldsymbol{C}^n$ も数ベクトルの加法に関して加法群である．明らかに $\boldsymbol{Z}^n$ は $\boldsymbol{C}^n$ の部分群である．

例題 1.1 整数の加法群 $\boldsymbol{Z}$(例 1.3 で $n=1$ の場合)を考える．$\boldsymbol{Z}\ni n$ に対して n の倍数の集合 $\{xn\,|\,x\in\boldsymbol{Z}\}$——これを $\langle n\rangle$ と書く——は $\boldsymbol{Z}$ の部分群である．逆に H を $\boldsymbol{Z}$ の任意の部分群とすれば，或る $n\in\boldsymbol{Z}$ が存在して $H=\langle n\rangle$ となる．H が単位群でなければ，n としては H に含まれる最小の正整数がとれる．

［証明］ 前半は容易であるから読者にまかせる．H を $\boldsymbol{Z}$ の任意の部分群とする．H が単位群ならば $H=\langle 0\rangle$ であるから正しい．よって H は単位群ではないとしてよい．このとき H は正整数を含む．なぜなら $H\ni x<0$ ならば $H\ni -x>0$ であるから．そこで n を H に含まれる最小の正整数としよう．$H\ni m$ を任意にとり，m を n で割って商を q，余りを r とすれば

$$m=qn+r \qquad (0\leqq r<n).$$

$m, qn\in H$ であるから，$r=m-qn\in H$．n の最小性により $r=0$ でなければならない．すなわち H の各元は n の倍数である．逆に $n\in H$ より n の任意の倍数は H に含まれるから，$H=\langle n\rangle$ を得る．▌

$\boldsymbol{Z}^n$ の部分群については第3章で述べる．

初等整数論でよく知られたつぎの命題は例題 1.1 の系である．これは以後ときどき用いられる．

例題 1.2 n 個の整数 $a_1,a_2,\cdots,a_n$ の最大公約数を d とする．不定方程式

$$a_1x_1+a_2x_2+\cdots+a_nx_n=b$$

が整数解をもつためには，b が d で割れることが必要十分である．とくに $a_1,a_2,\cdots,a_n$ が互いに素ならば，

$$a_1x_1+a_2x_2+\cdots+a_nx_n=1$$

は整数解をもつ．

［証明］ 必要であることは明らかである．十分であることを示すために，$d\,|\,b$

としよう．$H=\{a_1x_1+\cdots+a_nx_n \mid x_1, x_2, \cdots, x_n \in \boldsymbol{Z}\}$ とおくと，H は加法群 $\boldsymbol{Z}$ の部分群である．例題 1.1 により H は或る整数 d' の倍数の集合である：$H=\langle d'\rangle$. $d'=d$ を示せば証明は終る．$H \ni a_1, a_2, \cdots, a_n$ であるから，$d' \mid a_i$ $(i=1, 2, \cdots, n)$. 故に $d' \mid d$. 一方，$a_1x_1+\cdots+a_nx_n=d'$ を満たす $x_1, x_2, \cdots, x_n \in \boldsymbol{Z}$ が存在し，左辺は d で割れるから $d \mid d'$. したがって $d=d'$ である．▌

例 1.4 有限個の群 $G_1, G_2, \cdots, G_n$ が与えられたとき，直積集合 $G_1\times G_2\times\cdots\times G_n$ の上につぎのように演算が定義される：

$G_1\times G_2\times\cdots\times G_n \ni x=(x_1, x_2, \cdots, x_n)$，$y=(y_1, y_2, \cdots, y_n)$ に対し，

$$xy = (x_1y_1, x_2y_2, \cdots, x_ny_n).$$

この演算が結合法則を満たすことは明らかであろう．また e_i を G_i の単位元とすれば，$(e_1, e_2, \cdots, e_n)$ が $G_1\times G_2\times\cdots\times G_n$ の単位元であり，$x=(x_1, x_2, \cdots, x_n)$ の逆元は $(x_1^{-1}, x_2^{-1}, \cdots, x_n^{-1})$ である．したがって直積集合 $G_1\times G_2\times\cdots\times G_n$ は群となる．このようにして構成された群を，群 $G_1, G_2, \cdots, G_n$ の**直積**といい，$G_1\otimes G_2\otimes\cdots\otimes G_n$ と書く．$G_1, G_2, \cdots, G_n$ が加法群のときには，直積の演算も加法で書く：

$$x+y = (x_1+y_1, x_2+y_2, \cdots, x_n+y_n).$$

このときには直積という代りに**直和**とよばれ，$G_1\otimes\cdots\otimes G_n$ の代りに $G_1\oplus G_2\oplus\cdots\oplus G_n$ と書かれる．例 1.3 の $\boldsymbol{Z}^n$ や $\boldsymbol{C}^n$ はそれぞれ加法群 $\boldsymbol{Z}$ や $\boldsymbol{C}$ の n 個の直和にほかならない．

問 1.6 H_i を G_i の部分群とする $(1\leqq i\leqq n)$. $H_1\otimes H_2\otimes\cdots\otimes H_n$ は $G_1\otimes G_2\otimes\cdots\otimes G_n$ の部分群である．——

群 G の部分集合 S, T に対し

$$ST = \{st \mid s\in S,\ t\in T\}, \qquad S^{-1} = \{s^{-1} \mid s\in S\}$$

とおく．$G\supseteq S, T, U$ ならば，

$$(ST)U = S(TU), \qquad (ST)^{-1} = T^{-1}S^{-1} \tag{1.8}$$

である．

問 1.7 (1.8) を確かめよ．——

S, U がそれぞれただ一つの元 s, u から成るとき，

$$\{s\}T, \qquad T\{u\}, \qquad \{s\}T\{u\}$$

をそれぞれ簡単に

$$sT, \quad Tu, \quad sTu$$

と書く. $G \ni x$, $G \supseteqq S$ に対して

$$xSx^{-1}$$

の形の G の部分集合を S の**共役**という.

問 1.8 S, T を G の有限部分集合, $s, u \in G$ のとき

$$|ST| \leqq |S||T|, \qquad |sT| = |Ts| = |T|, \qquad |sTu| = |T|$$

を示せ. ここで $|X|$ は X に含まれる元の数を表わす.

問 1.9 部分群の共役は部分群であることを確かめよ. ——

G の部分群 H の共役がつねに H に等しいとき, すなわち

$$xHx^{-1} = H \qquad (\forall x \in G)$$

が成り立つとき, H を G の**正規部分群**といい,

$$G \triangleright H \quad \text{あるいは} \quad H \triangleleft G$$

と書く.

問 1.10 H を G の部分群とする. $xHx^{-1} \subseteqq H\ (\forall x \in G)$ ならば $G \triangleright H$ であることを示せ.

問 1.11 $G \supseteqq S$ のとき,

$$C_G(S) = \{x \in G \mid sx = xs\ (\forall s \in S)\},$$
$$N_G(S) = \{x \in G \mid xSx^{-1} = S\}$$

とおく. $C_G(S), N_G(S)$ は G の部分群であることおよび $N_G(S) \triangleright C_G(S)$ を示せ. $C_G(S)$ を S の G における**中心化群**, $N_G(S)$ を S の G における**正規化群**という.

問 1.12 $GL_n(\boldsymbol{C}) \triangleright SL_n(\boldsymbol{C})$, $\mathfrak{S}_n \triangleright \mathfrak{A}_n$, $GL_n(\boldsymbol{C}) \triangleright Z$ (Z は $GL_n(\boldsymbol{C})$ のスカラー行列の集合)を示せ. ——

つぎの補題はしばしば用いられる.

補題 1.1 H, K を G の部分群とする. HK が G の部分群であるためには, $HK = KH$ なることが必要十分である. H, K の少なくとも一方が G の正規部分群ならば, HK は G の部分群である.

証明 H, K は G の部分群だから

$$H = H^{-1}, \qquad K = K^{-1}, \qquad HH = H, \qquad KK = K$$

である. HK が G の部分群ならば,

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH$$

である．逆に $HK=KH$ ならば，(1.8)を用いて，

$$(HK)(HK)=H(KH)K=H(HK)K=(HH)(KK)=HK,$$
$$(HK)^{-1}=K^{-1}H^{-1}=KH=HK$$

となり，これらは HK が部分群であることを示す．よって補題の前半が証明された．H,K の一方たとえば H が G の正規部分群としよう．このとき $kHk^{-1}=H\ (\forall k\in K)$ より $kH=Hk\ (\forall k\in K)$，すなわち $KH=HK$ を得る．したがって補題の前半により HK は部分群である．▌

問 1.13　H_1, H_2, H_3 は G の部分群で，$H_i\subseteqq H_jH_k\ (i\neq j\neq k\neq i)$ ならば H_1H_2, H_2H_3, H_3H_1 は G の部分群であることを示せ．

§1.2　剰余類と剰余群

a）剰 余 類

H を G の部分群とする．$G\ni x,y$ に対して

$$(*)\qquad x^{-1}y\in H$$

なる関係は G の上の同値関係である．すなわち x,y が $(*)$ を満たすとき，$x\sim y$ と書けば，

(α)　$x\sim x$　(反射律)，

(β)　$x\sim y \Longrightarrow y\sim x$　(対称律)，

(γ)　$x\sim y,\ y\sim z \Longrightarrow x\sim z$　(推移律)

が成り立つ．

問 1.14　(α), (β), (γ) を確かめよ．——

$G\ni x$ を含む同値類 $\{y\in G\,|\,x\sim y\}$ は $(*)$ からわかるように xH である．xH を x を含む H の**左剰余類**という．また H の左剰余類の集合(＝同値関係$(*)$による商集合)を G/H と書く．H の各左剰余類から一つずつ元を選んで作った集合を H の**左剰余類の代表系**という．T を H の左剰余類の代表系とすれば

$$G=\bigcup_{t\in T}tH,\qquad tH\cap t'H=\phi\quad (t,t'\in T,\ t\neq t')$$

である．このことを

$$G=\sum_{t\in T}tH$$

と書き表わすこともある．同様にして，$G\ni x,y$ に対して

$$yx^{-1} \in H$$

なる関係は G の上の同値関係であり，x を含む同値類は Hx である．Hx を x を含む**右剰余類**といい，H の右剰余類の集合を $H\backslash G$ で表わす．T を H の右剰余類の代表系(H の各右剰余類から一つずつ元を選んで作った集合)とすれば

$$G = \sum_{t \in T} Ht.$$

くわしくは

$$G = \bigcup_{t \in T} Ht, \qquad Ht \cap Ht' = \phi \quad (t, t' \in T,\ t \neq t')$$

である．

$G \triangleright H$ ならば G の各元 x に対して

$$xHx^{-1} = H \quad \text{すなわち} \quad xH = Hx$$

であるから，右剰余類と左剰余類は一致し両者を区別する必要はない．したがって右剰余類(＝左剰余類)を単に**剰余類**とよぶ．

問 1.15 H を G の部分群，T を H の左剰余類の代表系とすれば，T^{-1} は H の右剰余類の代表系であることを示せ．とくに左剰余類の集合 G/H と右剰余類の集合 $H\backslash G$ は1対1に対応する．——

G の部分群 H に対して，H の左剰余類の数を $[G:H]$ で表わし G における H の**指数**という：

$$|G/H| = [G:H].$$

$[G:H]$ は有限とは限らないが，この記号が実質的に使用されるのは $[G:H]$ が有限のときである．上の問1.15より $[G:H]$ は右剰余類の数にも等しい：

$$|G/H| = [G:H] = |H\backslash G|.$$

つぎの定理は有限群の最初の著しい性質である．

定理 1.1(Lagrange) G を有限群，H をその部分群とすれば

$$|G| = [G:H] \cdot |H|.$$

とくに G の部分群の位数と指数は G の位数の約数である．

証明 xH を一つの左剰余類とすれば H から xH への写像

$$H \ni h \longmapsto xh \in xH$$

は全単射であるから，$|H| = |xH|$ すなわち H の各左剰余類は，$|H|$ 個の元を含む．一方 $[G:H]$ 個の左剰余類があるから，

$$|G| = [G:H]\cdot|H|$$

を得る. ▌

問 1.16 H, K を G の部分群で $H \supseteq K$ とする. このときつぎを示せ:

(i) $[G:K] = [G:H][H:K]$,

(ii) T を H の G における左剰余類の代表系, T' を K の H における左剰余類の代表系とすれば, TT' は K の G における左剰余類の代表系である.

問 1.17 H, K が G の有限部分群のとき, $|HK| = |H||K|/|H\cap K|$.

問 1.18 S を G の部分集合とする. S の異なる共役全体の集合と S の正規化群 $N_G(S)$ の左剰余類全体の集合 $G/N_G(S)$ は

$$xSx^{-1} \longleftrightarrow xN_G(S) \qquad (x \in G)$$

なる対応によって1対1に対応することを示せ. とくに G が有限群ならば, S の異なる共役の数は G の位数の約数である.

b) 剰余群

$G \triangleright N$ のとき, N の剰余類の集合 G/N に演算を定義して G/N がその演算に関して群になることを示そう. そのために最初に, 単位元1をもった半群とその上の或る同値関係が与えられたとき, それから群を構成する一つの簡単な原理を述べよう. この原理は自由群(第6章)やその他の群(本章例1.14)の構成にも用いられる.

補題 1.2 S は単位元1をもった半群で, S の上につぎの条件を満たす同値関係 $\sim$ が与えられているとする:

(i) $x \sim x',\ y \sim y' \Longrightarrow xy \sim x'y'$,

(ii) $S \ni \forall x,\quad S \ni \exists x',\quad xx' \sim 1$.

このとき, この同値関係による商集合 $\bar{S} = S/\sim$ は演算を自然に定義して群となる.

証明 $S \ni x$ に対して x を含む同値類を $\bar{x}$ で表わそう. このとき, $\bar{S} \ni \bar{x}, \bar{y}$ に対して

$$(*) \qquad \bar{x}\bar{y} = \overline{xy}$$

によって $\bar{S}$ の上に演算を定義することができる. それにはこの演算の定義が同値類の代表元のとり方によらないこと, すなわち

$$\bar{x} = \overline{x'},\quad \bar{y} = \overline{y'} \Longrightarrow \overline{xy} = \overline{x'y'}$$

を確かめなければならないが，上の条件(i)はこれが成り立つことにほかならない．S は半群であるから，$\bar{S}$ のこの演算も結合法則を満たす．また $\bar{1}$ は $\bar{S}$ の単位元であり，条件(ii)は $\bar{S}$ の各元が逆元をもつことを示す．したがって $\bar{S}$ は演算$(*)$に関して群になる．▌

$G \triangleright N$ としよう．G 上の同値関係 $x^{-1}y \in N$ が補題1.2の条件を満たすことを確かめよう．

$$x \sim x', \quad y \sim y' \quad \text{すなわち} \quad x^{-1}x' \in N, \quad y^{-1}y' \in N$$

とすると

$$(xy)^{-1}(x'y') = y^{-1}(x^{-1}x')y' = y^{-1}(x^{-1}x')y \cdot y^{-1}y'$$

において，$G \triangleright N$ および $x^{-1}x' \in N$ より $y^{-1}(x^{-1}x')y \in N$ であるから，これと $y^{-1}y' \in N$ より

$$(xy)^{-1}(x'y') \in N \quad \text{すなわち} \quad xy \sim x'y'$$

が得られる．したがって $x^{-1}y \in N$ なる同値関係は補題1.2の条件(i)が満たされている．条件(ii)は G が群であるから当然成り立っている．したがって補題1.2により，この同値関係の商集合 G/N は群になる．このように正規部分群 N を用いて構成された群 G/N を G の N による**剰余群**あるいは**商群**という．念のため剰余群 G/N の演算を書けば，

$$(xN)(yN) = xyN \qquad (xN, yN \in G/N) \tag{1.9}$$

となる．

例1.5 補題1.2の簡単な応用例をあげよう．n を1より大きい正整数とし，$\boldsymbol{Z}_n'$ を n と素な整数の集合とする：

$$\boldsymbol{Z}_n' = \{x \in \boldsymbol{Z} \mid (x, n) = 1\}.$$

$\boldsymbol{Z}_n'$ は整数の乗法に関して半群である．$\boldsymbol{Z}_n'$ の上の同値関係を

$$x \equiv y \pmod{n} \quad \text{すなわち} \quad n \mid x-y$$

によって定義するとこれは補題1.2の条件(i),(ii)を満たす．

問1.19 これを確かめよ．((ii)を確かめるとき例題1.2を用いる．) ——

したがって商集合 $\boldsymbol{Z}_n^*$ は群になる．$\varphi(n)$ を $1, 2, \cdots, n-1$ のうち n と素なものの個数とすれば，$\boldsymbol{Z}_n^*$ は位数 $\varphi(n)$ の Abel 群である．$\varphi(n)$ は **Euler 関数**とよばれる有名な関数であり，本書でもしばしば登場するであろう．

問1.20 補題1.2において S を群，$\sim$ を(i),(ii)を満たす同値関係とする．

このとき S の正規部分群 N が存在して

$$x \sim y \Longleftrightarrow x^{-1}y \in N$$

となることを示せ．すなわち S が群のときは，$\bar{S}$ は S のある正規部分群による剰余群にほかならない．

例 1.6　(i)　整数の加法群 $\boldsymbol{Z}$ の任意の部分群は，或る整数 n の倍数の集合 $\langle n\rangle$ であった(例題 1.1)．$\boldsymbol{Z}$ の $\langle n\rangle$ による剰余群 $\boldsymbol{Z}/\langle n\rangle$ を $\boldsymbol{Z}_n$ で表わす．$n>0$ ならば $\boldsymbol{Z}_n$ は位数 n の Abel 群である．

(ii)　$Z_n(\boldsymbol{C})=\{\alpha E_n \mid \alpha \in \boldsymbol{C}^*\}$ は，$GL_n(\boldsymbol{C})$ の正規部分群である．$GL_n(\boldsymbol{C})$ の $Z_n(\boldsymbol{C})$ による剰余群を **$n-1$ 次元射影線型群**(n 次元ではない！)といい，$PGL_n(\boldsymbol{C})$ と書く：

$$PGL_n(\boldsymbol{C}) = GL_n(\boldsymbol{C})/Z_n(\boldsymbol{C}).$$

また $SL_n(\boldsymbol{C}) \triangleright SL_n(\boldsymbol{C}) \cap Z_n(\boldsymbol{C})$ である．$SL_n(\boldsymbol{C}) \cap Z_n(\boldsymbol{C})$ による $SL_n(\boldsymbol{C})$ の剰余群を $PSL_n(\boldsymbol{C})$ で表わし，**$n-1$ 次元射影特殊線型群**という．

§1.3　準同型写像

a)　準同型と同型

G, G' を群とする．G から G' への写像 f が

(1.10)　　$$f(xy) = f(x)f(y) \qquad (\forall x, y \in G)$$

なる条件を満たすとき，f を G から G' への**準同型写像**あるいは簡単に**準同型**という．f が全射のとき G から G' の**上への**準同型(写像)，単射のとき G から G' の**中への**同型(写像)，全単射のとき G から G' の**上への**同型(写像)という．また G から G' の上への同型が存在するとき，G と G' は**同型**であるといい，

$$G \simeq G'$$

と書く．

$G \triangleright N$ として，$G \ni x$ を含む N の剰余類を $\bar{x}$ と書けば，剰余群 G/N の積の定義(1.9)からわかるように G から G/N への写像

$$G \ni x \longmapsto \bar{x} \in G/N$$

は G から G/N の上への準同型である．この準同型を G から G/N への**標準的準同型**あるいは**自然準同型**という．一般に f を G から G' への準同型とするとつぎのことが容易にわかる：

(α) $f(1)=1'$ ($1, 1'$ はそれぞれ G, G' の単位元),

(β) $f(x^{-1})=f(x)^{-1}$ ($\forall x \in G$),

(γ) f による G の像 $f(G)=\{f(x) \mid x \in G\}$ は G' の部分群,

(δ) G' の単位元 $1'$ の逆像 $f^{-1}(1')=\{x \in G \mid f(x)=1'\}$ は G の正規部分群である．$f^{-1}(1')$ を f の**核**といい，$\mathrm{Ker}\, f$ で表わす．

問 1.21 (α), (β), (γ), (δ) を証明せよ．

問 1.22 つぎを示せ：(i) $G \simeq G$, (ii) $G \simeq G' \Longrightarrow G' \simeq G$, (iii) $G \simeq G'$, $G' \simeq G'' \Longrightarrow G \simeq G''$.

問 1.23 実数の加法群 $\boldsymbol{R}$ と正の実数の乗法群は同型である．同型写像は何か．

問 1.24 $\mathfrak{S}(\Omega)$ を §1.1 例 1.2 の通りとする．(1.4), (1.4)$'$ によって $\mathfrak{S}(\Omega)$ には 2 通りの演算が定義される．これら二つの群は同型であることを示せ．

例 1.7 合同変換群 $\boldsymbol{R}^n$ を実数を成分とする n 項行ベクトルの集合とする．$\boldsymbol{R}^n \ni x=(x_1, x_2, \cdots, x_n)$, $y=(y_1, y_2, \cdots, y_n)$ に対して

$$(x, y)=\sum_{i=1}^{n} x_i y_i$$

によって内積を定義する．この内積を考え合わせたとき $\boldsymbol{R}^n$ を n **次元 Euclid 空間**という．$\boldsymbol{R}^n \ni x, y$ に対して x と y の間の距離 $d(x, y)$ は

$$d(x, y)=\sqrt{\sum_{i=1}^{n}(x_i-y_i)^2}=\sqrt{(x-y, x-y)} \qquad \begin{pmatrix} x=(x_1, x_2, \cdots, x_n), \\ y=(y_1, y_2, \cdots, y_n) \end{pmatrix}$$

によって定義される．

さて $\boldsymbol{R}^n$ から $\boldsymbol{R}^n$ への全単射 f (例 1.2 の記号で $\mathfrak{S}(\boldsymbol{R}^n)$ の元) が

$$d(f(x), f(y))=d(x, y) \qquad (\forall x, y \in \boldsymbol{R}^n)$$

を満たすとき，f を $\boldsymbol{R}^n$ の**合同変換**という．$\boldsymbol{R}^n$ の合同変換の集合を $I(\boldsymbol{R}^n)$ と書く：

$$I(\boldsymbol{R}^n)=\{f \in \mathfrak{S}(\boldsymbol{R}^n) \mid d(f(x), f(y))=d(x, y)\ (\forall x, y \in \boldsymbol{R}^n)\}.$$

このとき

(i) $I(\boldsymbol{R}^n)$ は $\mathfrak{S}(\boldsymbol{R}^n)$ の部分群である．

$\boldsymbol{R}^n \ni a$ に対して

$$f_a(x)=x+a \qquad (x \in \boldsymbol{R}^n)$$

によって $\boldsymbol{R}^n$ から $\boldsymbol{R}^n$ への写像 f_a を定義すると，これは $\boldsymbol{R}^n$ の合同変換である：

$$f_a \in I(\boldsymbol{R}^n).$$

(ii)　$T(\boldsymbol{R}^n)=\{f_a \mid a\in \boldsymbol{R}^n\}$ とおくと，$T(\boldsymbol{R}^n)$ は $I(\boldsymbol{R}^n)$ の正規部分群である：

$$I(\boldsymbol{R}^n) \triangleright T(\boldsymbol{R}^n).$$

$T(\boldsymbol{R}^n)$ を $\boldsymbol{R}^n$ の**平行移動の群**という．

(iii)　$\boldsymbol{R}^n$ から $T(\boldsymbol{R}^n)$ への写像

$$a \longmapsto f_a$$

は，$\boldsymbol{R}^n$ から $T(\boldsymbol{R}^n)$ の上への同型である：

$$\boldsymbol{R}^n \simeq T(\boldsymbol{R}^n).$$

(iv)　また $A\in O(n)$ (n 次実直交群) に対して

$$f_A(x) = x^t A$$

によって $\boldsymbol{R}^n$ から $\boldsymbol{R}^n$ への写像を定義すると，$f_A\in I(\boldsymbol{R}^n)$ である．

(v)　$O_1(n)=\{f_A \mid A\in O(n)\}$ とおくと，$O_1(n)$ は $I(\boldsymbol{R}^n)$ の部分群である．

(vi)　また，

$$A \longmapsto f_A$$

なる写像は，$O(n)$ から $O_1(n)$ の上への同型である：

$$O(n) \simeq O_1(n).$$

この同型によって $O_1(n)$ と $O(n)$ を同一視して以後 $O_1(n)$ を $O(n)$ と書く．ところで $f\in I(\boldsymbol{R}^n)$ が原点 $O=(0,0,\cdots,0)$ を動かさなければ，$f\in O(n)$ であることが証明できる：

(vii)　$O(n) = \{f\in I(\boldsymbol{R}^n) \mid f(O)=O\}$.

これから

(viii)　$I(\boldsymbol{R}^n) = O(n)\cdot T(\boldsymbol{R}^n),\quad O(n)\cap T(\boldsymbol{R}^n) = 1$

がわかる．したがって任意の合同変換は，直交変換と平行移動の積に(一意的に)書ける．なお $SO(n)\cdot T(\boldsymbol{R}^n)$ の元を $\boldsymbol{R}^n$ の**運動**ということがある．とくに $n=2,3$ のとき，線型代数で周知のように $SO(2), SO(3)$ の元は原点 O を中心とする回転を表わすから，$SO(2), SO(3)$ をそれぞれ**2次元回転群**，**3次元回転群**という．

問 1.25　(i)-(viii) を証明せよ．

例 1.8　正多面体群　3次元 Euclid 空間に5個の正多面体——正 4, 6, 8, 12, 20 面体——のあることが知られている．

正 n 面体 ($n=4,6,8,12,20$) の中心を原点 O として，O を中心とする回転で正

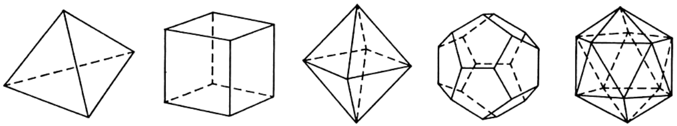


図1

n 面体を自分自身に重ね合わすもの全体は群を作る($SO(3)$ の部分群!). これを $P(n)$ で表わすとき,

(i) $P(6) \simeq P(8)$,　$P(12) \simeq P(20)$.

正6面体と正8面体は, それぞれ一方のとなり合った面の中心を結べば他方の多面体が得られる. 正12面体と正20面体についても同じである. これから上の同型は明らかであろう.

(ii) $P(4) \simeq \mathfrak{A}_4$ (4次交代群), $P(6) \simeq \mathfrak{S}_4$ (4次対称群), $P(12) \simeq \mathfrak{A}_5$ (5次交代群) であることが知られている. $P(4) \simeq \mathfrak{A}_4$ は, $P(4)$ の元にそれがひき起す正4面体の四つの頂点の間の置換を対応させることによって得られる. $P(6) \simeq \mathfrak{S}_4$ は, $P(6)$ の各元にそれがひき起す正6面体の4本の対角線の間の置換を対応させることによって得られる. しかし $P(12) \simeq \mathfrak{A}_5$ については, このような直観的対応はなく少し難しくなるのでここでは省略する.

問 1.26　(ii)に示された対応で $P(4) \simeq \mathfrak{A}_4$, $P(6) \simeq \mathfrak{S}_4$ であることを確かめよ.

b) 同型定理

準同型と剰余群の関係を示すつぎの三つの定理は群論においてしばしば用いられる.

定理 1.2 (準同型定理)　f を G から G' の上への準同型とすれば,

$$G/\mathrm{Ker}\, f \simeq G'.$$

証明　$\mathrm{Ker}\, f = \{x \in G \mid f(x) = 1'\}$ ($1'$ は G' の単位元) であった. これを N と書き, 剰余群 G/N の元 xN を $\bar{x}$ と書く. $\bar{x}$ に G' の元 $f(x)$ を対応させる写像 $\bar{f}$ を考える:

$$\bar{f}(\bar{x}) = f(x).$$

この定義が剰余類 xN の代表元 x のとり方によらないこと, すなわち

$$\bar{x} = \bar{y} \Longrightarrow f(x) = f(y)$$

を確かめねばならないが，それは

$$\bar{x} = \bar{y} \Leftrightarrow x^{-1}y \in N \Leftrightarrow 1' = f(x^{-1}y) = f(x)^{-1}f(y)$$
$$\Leftrightarrow f(x) = f(y)$$

からわかる．またこれは $\bar{f}$ が単射であることも示している．f は全射だから明らかに $\bar{f}$ も全射であり，結局 $\bar{f}$ は G/N から G' への全単射である．最後に $\bar{f}$ が準同型であることは，

$$\bar{f}(\bar{x}\bar{y}) = \bar{f}(\overline{xy}) = f(xy) = f(x)f(y) = \bar{f}(\bar{x})\bar{f}(\bar{y})$$

からわかる．▌

定理 1.3（**第1同型定理**） f を G から G' の上への準同型，N' を G' の正規部分群とする．$N=f^{-1}(N')$ $(=\{x \in G \mid f(x) \in N'\})$ とおくと，N は G の正規部分群で $G/N \simeq G'/N'$.

証明 φ' を G' から G'/N' への自然準同型とする．G から G'/N' の上への写像 $\varphi' f$

$$G \xrightarrow{f} G' \xrightarrow{\varphi'} G'/N'$$

は G から G'/N' の上への準同型である．準同型 $\varphi' f$ の核は $N=f^{-1}(N')$ にほかならないから，準同型定理により

$$G/N \simeq G'/N'$$

を得る．▌

定理 1.4（**第2同型定理**） H, N を G の部分群，N を G の正規部分群とすると，

$$HN/N \simeq H/H \cap N.$$

証明 最初に補題1.1により HN が G の部分群であることに注意する．H から HN/N への写像

$$H \ni h \longmapsto hN \in HN/N$$

は H から HN/N の上への準同型であり，その核は $H \cap N$ である．したがって準同型定理により

$$H/H \cap N \simeq HN/N$$

を得る．▌

問 1.27 f を G から G' への準同型，N は G の正規部分群，φ を G から G/N の上への自然準同型とする．$\mathrm{Ker}\, f \supseteq N$ ならば，G/N から G' への準同型 g で $g\varphi$

$=f$ となるものがただ一つ存在することを示せ．すなわち下の図式が可換となる g が $(\mathrm{Ker}\, f \supseteqq N$ なる仮定のもとで$)$存在して一意的であることを示すのである．

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & \searrow^{\varphi} \quad \nearrow_{g} & \\ & G/N & \end{array}$$

問 1.28　$G_i \triangleright N_i$ $(i=1,2,\cdots,n)$ のとき，$(G_1\otimes\cdots\otimes G_n)/(N_1\otimes\cdots\otimes N_n)\simeq G_1/N_1 \otimes\cdots\otimes G_n/N_n$．——

群 G から G の上への同型を G の**自己同型**という．G のすべての自己同型の集合は写像の積に関して群となる．これを G の**全自己同型群**といい，$\mathrm{Aut}\,(G)$ で表わす．$\mathrm{Aut}\,(G)$ の部分群を**自己同型群**という．$G \ni y$ に対して G から G への写像

$$x \longmapsto yxy^{-1}$$

は G の自己同型である．このような自己同型を G の**内部自己同型**という．内部自己同型の全体は $\mathrm{Aut}\,(G)$ の部分群を作り，これを $\mathrm{Inn}\,(G)$ で表わす．また

$$Z(G)=\{x\in G \mid xy=yx\ (\forall y\in G)\}$$

とおくと，$Z(G)$ は G の可換な正規部分群である．$Z(G)$ を G の**中心**という．

問 1.29　$\mathrm{Aut}\,(G)\triangleright \mathrm{Inn}\,(G)$，$\mathrm{Inn}\,(G)\simeq G/Z(G)$ を示せ．

§1.4 巡 回 群

群 G の元 a の n 個の積を a^n と書く：

$$a^n = \underbrace{aa\cdots a}_{n}.$$

さらに整数 0 および負の整数 $-n$ $(n>0)$ に対して

$$a^0 = 1,$$
$$a^{-n} = (a^{-1})^n \qquad (\text{右辺は } a \text{ の逆元 } a^{-1} \text{ の } n \text{ 個の積})$$

と定義する．このとき指数法則

(i)　$(a^m)^n = a^{mn}$,

(ii)　$a^{m+n} = a^m\cdot a^n$

が任意の整数 m,n に対して成り立つ．

問 1.30　指数法則 (i), (ii) を確かめよ．また $b^{-1}a^n b=(b^{-1}ab)^n$ $(a,b\in G,\ n\in$

$\boldsymbol{Z}$)を示せ. ——

$G \ni a$ のベキ全体の集合を $\langle a\rangle$ と書く:

$$\langle a\rangle = \{a^n \mid n \in \boldsymbol{Z}\}.$$

指数法則により $\langle a\rangle$ は G の部分群である. このような部分群は a によって生成される**巡回部分群**とよばれる. 整数の加法群 $\boldsymbol{Z}$ から巡回部分群 $\langle a\rangle$ への写像

$$\boldsymbol{Z} \ni m \longmapsto a^m \in \langle a\rangle$$

は, 再び指数法則により $\boldsymbol{Z}$ から $\langle a\rangle$ の上への準同型である. その核 $\{m \in \boldsymbol{Z} \mid a^m = 1\}$ は例題1.1により或る整数 n_a ($n_a \geqq 0$) の倍数全体の作る $\boldsymbol{Z}$ の部分群 $\langle n_a\rangle$ に等しい:

$$\langle n_a\rangle = \{m \in \boldsymbol{Z} \mid a^m = 1\}. \tag{1.11}$$

このとき準同型定理により

$$\boldsymbol{Z}_{n_a} = \boldsymbol{Z}/\langle n_a\rangle \simeq \langle a\rangle \tag{1.12}$$

である.

一般に $a^n = 1$ なる正整数 n が存在するとき, a は**位数有限**であるといい, このような最小の正整数 n を a の**位数**という. (1.11)により a が位数有限であるためには, $n_a > 0$ なることが必要十分であり, このとき n_a が a の位数となる. また(1.12)により a の位数は部分群 $\langle a\rangle$ の位数に等しい. 以上からつぎの補題は明らかである.

補題 1.3 つぎの条件は同値である:

(i) a は位数有限,

(ii) $a^p = a^q \quad (\exists p, q \in \boldsymbol{Z},\ p \neq q)$,

(iii) $\langle a\rangle$ が有限集合.

このとき, a の位数は部分群 $\langle a\rangle$ の位数に等しい.

例 1.9 有限群の各元は位数有限である. これは補題1.3から明らかである. また補題1.3と定理1.1により, 有限群の元の位数は群の位数の約数である. とくに有限群 G の任意の元 x に対して

$$x^{|G|} = 1 \tag{1.13}$$

である. (1.13)を例1.5で構成された位数 $\varphi(n)$ の Abel 群 $\boldsymbol{Z}_n{}^*$ に適用すれば, 初等整数論でよく知られた **Fermat の小定理**が得られる. すなわち $\boldsymbol{Z} \ni n > 0$, a が n と素のとき

$$a^{\varphi(n)} \equiv 1 \pmod n$$

である．とくに $n=p$ が素数ならば $\varphi(p)=p-1$ であるから

$$a^{p-1} \equiv 1 \pmod p$$

となる．

補題 1.4 $G \ni a$ の位数を n_a とする．a^m の位数は $n_a/(m, n_a)$ である．ここで (m, n_a) は m と n_a の最大公約数を表わす．とくに $a^m=1$ であるためには m が n_a の倍数であることが必要十分である．

証明 a^m の位数を p，$p'=n_a/(m, n_a)$ とする．$a^{mp}=1$ だから，(1.11) により $n_a | mp$，したがって $p'|p$ である．一方 $n_a | mp'$ より $a^{mp'}=1$，a^m の位数は p だから $p|p'$．したがって $p=p'$ でなければならない．▌

問 1.31 Abel 群の位数有限の元の集合は部分群であることを示せ．

問 1.32 $G \ni a, b$ のそれぞれの位数を m, n とする．m と n が互いに素で $ab=ba$ ならば，ab の位数は mn であることを示せ．

問 1.33 $G_1, G_2, \cdots, G_n$ を群，a_i を G_i の位数 m_i の元とする．$G_1 \otimes G_2 \otimes \cdots \otimes G_n$ の元 $(a_1, a_2, \cdots, a_n)$ の位数は，$m_1, m_2, \cdots, m_n$ の最小公倍数であることを示せ．——

なお，G が加群のときは，a の n 乗 a^n に対応して，a の n 倍が定義される．すなわち正整数 n に対しては，

$$na = \underbrace{a+a+\cdots+a}_{n}$$

であり，整数 0 および負の整数 $-n$ $(n>0)$ に対しては

$$0a = 0 \qquad \text{(右辺は加群の零元)},$$
$$(-n)a = n(-a)$$

とするのである．指数法則は

$$\begin{aligned} m(na) &= (mn)a, \\ (m+n)a &= ma+na \end{aligned} \qquad (m, n \in \boldsymbol{Z})$$

となる．

或る $a \in G$ が存在して $G=\langle a\rangle$ となるとき G を**巡回群**という．このとき a を巡回群 G の**生成元**という．加法群 $\boldsymbol{Z}$ は整数 1 を生成元とする無限巡回群である．(1.12) により任意の巡回群は $\boldsymbol{Z}$ の準同型像であり，その位数が n ならばそれは

$\boldsymbol{Z}_n$ と同型である.

定理 1.5　G を巡回群とする.

(i)　G の部分群は巡回群である.

(ii)　G が有限巡回群のとき, $|G|$ の各約数 m に対し位数 m の部分群がただ一つ存在する.

(iii)　a を G の生成元とする: $G=\langle a\rangle$. G が無限巡回群ならば生成元は a または a^{-1} に限る. G が位数 n の巡回群ならば, a^m が G の生成元であるためには, m と n が互いに素であることが必要十分である.

証明　(i) (1.12) により巡回群 $\langle a\rangle$ の部分群は $\boldsymbol{Z}$ の或る部分群の準同型像である. また例題 1.1 により $\boldsymbol{Z}$ の任意の部分群は巡回群である. 一方, 巡回群の準同型像が巡回群であることは明らかであるから, 巡回群 $\langle a\rangle$ の任意の部分群は巡回群でなければならない. (ii) $G=\langle a\rangle$ を位数 n の巡回群とする. 再び (1.12) により n の各約数 m に対し $\boldsymbol{Z}$ の指数 n/m の部分群が存在してただ一つであることをいえば十分である. しかるに $\langle n/m\rangle$ はたしかに $\boldsymbol{Z}$ の指数 n/m の部分群であり, 例題 1.1 によりそのような部分群は $\langle n/m\rangle$ に限る. (iii) G が無限巡回群とすると補題 1.3 により

$$a^p = a^q \Leftrightarrow p = q$$

である. a^i が G の生成元とすると, $a^{ij}=a$ $(\exists j\in\boldsymbol{Z})$, したがって $ij=1$. これから $i=\pm 1$ がでる. G を位数 n の巡回群とすると

$$\begin{aligned} G = \langle a^i\rangle &\Leftrightarrow a^i \text{ の位数が } n \\ &\Leftrightarrow n = n/(i,n) \qquad (\text{補題 } 1.4) \\ &\Leftrightarrow (i,n) = 1 \end{aligned}$$

である. ▮

$\varphi(n)$ を Euler 関数 (すなわち $1,2,\cdots,n-1$ のうち n と素なものの数) とすると, 定理 1.5 (iii) により

$$\varphi(n) = (\text{位数 } n \text{ の巡回群の生成元の数})$$

であることがわかる. このことから Euler 関数のよく知られた性質——例題 1.3——および巡回群の一つの特徴づけ——例題 1.4——が得られる.

例題 1.3　$\sum_{d|n}\varphi(d) = n$.

[証明]　G を位数 n の巡回群, G の位数 d の元の集合を C_d とする. $d|n$ に

注意して

$$(*) \qquad \sum_{d|n} |C_d| = n$$

である．ところで C_d の各元は位数 d の部分群 G_d を生成し，定理1.5(ii)により G の位数 d の部分群はただ一つしか存在しないから，C_d は位数 d の巡回群 G_d の生成元の全体にほかならない．よって

$$(**) \qquad |C_d| = \varphi(d).$$

(*)と(**)から $\sum_{d|n} \varphi(d) = n$ を得る．▌

例題 1.4 G を有限群とする．G が，各正整数 d に対して $x^d=1$ を満たす元を高々 d 個しか含まなければ，G は巡回群である．

［証明］ $|G|=n$ として，位数 n の元の存在をいえばよい．正整数 d に対して G の位数 d の元の数を $\psi(d)$ とする．$d \nmid n$ ならば $\psi(d)=0$ だから，

$$\sum_{d|n} \psi(d) = n.$$

δ を位数 d の元とすると，$1, \delta, \delta^2, \cdots, \delta^{d-1}$ は $x^d=1$ を満たすから，仮定により位数 d の元は $\langle\delta\rangle = \{1, \delta, \cdots, \delta^{d-1}\}$ に含まれる．これは n の各約数 d に対して

$$\psi(d) = \varphi(d) \quad \text{または} \quad 0$$

を示すから，

$$n = \sum_{d|n} \psi(d) \leqq \sum_{d|n} \varphi(d) = n.$$

したがって n の各約数に対して $\psi(d)=\varphi(d)$．とくに $\psi(n)=\varphi(n)$．したがって位数 n の元が存在する．▌

問 1.34 複素数体の乗法群 $\boldsymbol{C}^*$ の有限部分群は巡回群である．(一般に体の乗法群の有限部分群は巡回群である．§1.7 定理1.10参照.)

問 1.35 $\mathrm{Aut}(\boldsymbol{Z}) \simeq \boldsymbol{Z}_2$，$\mathrm{Aut}(\boldsymbol{Z}_n) \simeq \boldsymbol{Z}_n^*$ $(n>0)$ を示せ．ここで $\boldsymbol{Z}_n^*$ は例1.5の群である．——

つぎの例題1.5は例題1.2の系である．これを用いて例1.5で構成された Abel 群 $\boldsymbol{Z}_n^*$ の直積分解を与えよう．

例題 1.5 $n = m_1 m_2 \cdots m_t$ (n, m_i は正整数)，$m_1, m_2, \cdots, m_t$ のどの二つも互いに素とする．$\boldsymbol{Z} \ni x_1, x_2, \cdots, x_t$ に対し

$$(*) \qquad x \equiv x_i \pmod{m_i} \qquad (i=1, 2, \cdots, t)$$

を満たす x が $\mathrm{mod}\, n$ で一意的である．

[証明] (*)を満たす解の mod n での一意性(すなわち x, x' がともに(*)を満たせば $x \equiv x' \pmod{n}$)は明らかである. t に関する数学的帰納法で解の存在を示そう. $t=1$ のときは証明すべきことは何もない. $n'=m_1m_2\cdots m_{t-1}$ とおくと数学的帰納法の仮定により

$$(**) \qquad x' \equiv x_i \pmod{m_i} \qquad (1 \leqq i \leqq t-1)$$

を満たす $x' \in \boldsymbol{Z}$ が存在する. n' と m_t は互いに素だから例題1.2により

$$n'u - m_t v = x_t - x'$$

を満たす整数 u, v が存在する. このとき

$$x = x_t + m_t v = x' + n'u$$

とおくと,

$$x \equiv x_t \pmod{m_t}, \qquad x \equiv x' \pmod{n'}$$

である. このとき(**)と合わせて

$$x \equiv x_i \pmod{m_i} \qquad (1 \leqq i \leqq t)$$

を得る. ▌

定理 1.6 $\boldsymbol{Z}_n{}^*$ を例1.5で構成された位数 $\varphi(n)$ の Abel 群, $n=p_1{}^{e_1}p_2{}^{e_2}\cdots p_t{}^{e_t}$ を n の素因子分解とする. このとき

$$(1.14) \qquad \boldsymbol{Z}_n{}^* \simeq \boldsymbol{Z}_{q_1}{}^* \otimes \boldsymbol{Z}_{q_2}{}^* \otimes \cdots \otimes \boldsymbol{Z}_{q_t}{}^* \qquad (q_i = p_i{}^{e_i})$$

である. とくに Euler 関数に対して

$$\varphi(n) = \varphi(p_1{}^{e_1})\varphi(p_2{}^{e_2})\cdots\varphi(p_t{}^{e_t})$$

が成り立つ.

証明 $\boldsymbol{Z}_n{}^*$ から $\boldsymbol{Z}_{q_1}{}^* \otimes \cdots \otimes \boldsymbol{Z}_{q_t}{}^*$ $(q_i = p_i{}^{e_i})$ への自然な写像

$$\boldsymbol{Z}_n{}^* \ni \bar{x} \longmapsto (\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_t) \in \boldsymbol{Z}_{q_1}{}^* \otimes \cdots \otimes \boldsymbol{Z}_{q_t}{}^*$$

を考える. ここで $\bar{x}_i$ は, x を含む $\boldsymbol{Z}_{q_i}{}'$(記号の意味は例1.5参照)の同値類を表わす. この写像が準同型であることを見るのはまったく易しい. ところで $m_i = p_i{}^{e_i}$ $(1 \leqq i \leqq t)$ として前例題を適用すれば, それはこの写像が全単射であることを示している. したがって(1.14)を得る. ▌

§1.5 生成系

S を群 G の部分集合とする. G の S を含むすべての部分群の共通部分は G の部分群である. これを S で生成される G の部分群といい, $\langle S \rangle$ で表わす:

$$\langle S\rangle = \bigcap_{\lambda} H_\lambda \qquad (H_\lambda \text{ は } S \text{ を含むすべての部分群を走る}).$$

$\langle S\rangle$ は G の S を含む最小の部分群であるといってもよい．また容易にわかるように

$$\begin{aligned}\langle S\rangle &= \{a_1a_2\cdots a_n \mid a_i\in S\cup S^{-1},\ n=1,2,\cdots\}\\ &= \{s_1^{n_1}s_2^{n_2}\cdots s_t^{n_t} \mid s_i\in S,\ n_i\in \boldsymbol{Z}\}\end{aligned}$$

である．

問 1.36 これを確かめよ．——

$G=\langle S\rangle$ のとき，S を G の**生成系**，S の元を G の**生成元**という．G が有限個の元からなる生成系をもつとき，G は**有限生成**であるという．ただ一つの元から生成される群は巡回群にほかならない．明らかに群の生成系は一意的に定まるものではないが，わかり易い生成系を取ったり，その群を調べる目的に応じて都合のよい生成系を取ることが大切である．

例 1.10 n 次対称群 $\mathfrak{S}_n$ の任意の置換は互換の積 (例 1.2, (1.6)) であるから，すべての互換の集合は $\mathfrak{S}_n$ の生成系である．また交代群の定義により，二つの互換の積全体の集合は交代群 $\mathfrak{A}_n$ の生成系である．ところで一般に

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l) \qquad (i,j,k,l \text{ は互いに異なる文字})$$

なる等式が成り立つから，長さ 3 の巡回置換の全体も $\mathfrak{A}_n$ の生成系である．

問 1.37 $n-1$ 個の互換 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ は $\mathfrak{S}_n$ の生成系であることを示せ．[ヒント] $(j\ l)(i\ j)(j\ l)=(i\ l)$.

例 1.11 つぎの形の n 次正則行列を考える：

$$P_{(i,j)} = \begin{bmatrix} 1 & & & \vdots & & & & \vdots & & & \\ & \ddots & & \vdots & & & & \vdots & & & \\ & & 1 & \vdots & & & & \vdots & & & \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 1 & \cdots & \cdots & \cdots \\ & & & \vdots & 1 & & & \vdots & & & \\ & & & \vdots & & \ddots & & \vdots & & & \\ & & & \vdots & & & 1 & \vdots & & & \\ \cdots & \cdots & \cdots & 1 & \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ & & & \vdots & & & & \vdots & 1 & & \\ & & & \vdots & & & & \vdots & & \ddots & \\ & & & \vdots & & & & \vdots & & & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \\ \end{matrix},$$

（第 i 列，第 j 列）

$$Q(i,c)=\begin{bmatrix}1&&&\vdots&&&\\&\ddots&&\vdots&&&\\&&1&\vdots&&&\\\cdots&\cdots&\cdots&c&\cdots&\cdots&\cdots\\&&&\vdots&1&&\\&&&\vdots&&\ddots&\\&&&\vdots&&&1\end{bmatrix}i,\quad (c\neq 0) \qquad R(i,j,c)=\begin{bmatrix}1&&\vdots&&\vdots&&\\&\ddots&\vdots&&\vdots&&\\\cdots&\cdots&1&\cdots&c&\cdots&\cdots\\&&\vdots&\ddots&\vdots&&\\\cdots&\cdots&&\cdots&1&\cdots&\cdots\\&&\vdots&&\vdots&\ddots&\\&&\vdots&&\vdots&&1\end{bmatrix}\begin{matrix}\\\\i\\\\j\\\\\\\end{matrix},\quad (i\neq j)$$

このような形の(複素数成分の)行列全体を S とすると，S は $GL_n(\boldsymbol{C})$ の生成系である．成分を実数に限れば(すなわち $Q(i,c)$，$R(i,j,c)$ において $c\in\boldsymbol{R}$ に限れば)，$GL_n(\boldsymbol{R})$ の生成系である．これは行列の基本変形の理論からの帰結である．すなわち任意の n 次行列 A は，上の形のいくつかの行列を左右から掛けて

$$UAV=\begin{bmatrix}E_r&0\\0&0\end{bmatrix}\qquad (r=A \text{ の階数},\ U,V \text{ は } S \text{ の元の積})$$

の形になる．(§3.1で同じことをするので参照せよ.) とくに A が正則行列ならば $r=n$ であるから

$$A=U^{-1}V^{-1}$$

となり，A は S の元の積として書ける．($S=S^{-1}$ に注意.)

問 1.38 $GL_n(\boldsymbol{C})$ は，$Q(i,c)$，$R(i,j,c)$ の形の行列だけで生成される．また $SL_n(\boldsymbol{C})$ は $R(i,j,c)$ の形の行列で生成される．

[ヒント]　$\begin{bmatrix}0&1\\-1&0\end{bmatrix}=\begin{bmatrix}1&0\\-1&1\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\-1&1\end{bmatrix}.$

例 1.12 実直交群 $O(n)$ の生成系としてはつぎのものが有名である．例1.7におけるように $O(n)$ を n 次元 Euclid 空間 $\boldsymbol{R}^n$ の合同変換群の部分群(すなわち原点を不変にする合同変換の全体)と考える．したがって

$$O(n)=\{f_A\mid A\in O(n)\},\qquad f_A(x)=x^tA\quad (x\in\boldsymbol{R}^n)$$

である．$\boldsymbol{R}^n\ni a$ に対して $\boldsymbol{R}^n$ から $\boldsymbol{R}^n$ への写像 r_a を

$$r_a(x)=x-\frac{2(x,a)}{(a,a)}a$$

によって定義すると，

(i)　$r_a\in O(n)$，　${r_a}^2=1$

である．幾何学的にいうと，r_a は

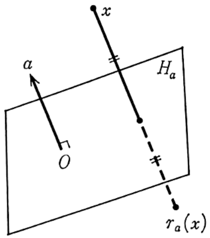


図 2

$$H_a = \{x \in \boldsymbol{R}^n \mid (x, a) = 0\}$$

によって定義される超平面に関する折返しである．r_a を超平面 H_a に関する**鏡映**という．さて

$$R = \{r_a \mid 0 \neq a \in \boldsymbol{R}^n\}$$

は，$O(n)$ の生成系である．それを見るにはつぎのことに注意するとよい：

(ii) $x_1, x_2, \cdots, x_n$ を $\boldsymbol{R}^n$ の正規直交基底とする．$A \in O(n)$ が

$$f_A(x_i) = x_i \qquad (1 \leqq i \leqq k-1),$$
$$f_A(x_k) = x_k' \neq x_k$$

であるとき，$f_{A'} = r_{x_k'-x_k} f_A$ とおくと，$f_{A'}(x_i) = x_i$ $(1 \leqq i \leqq k)$ となる．

これを用いて R が $O(n)$ の生成系であることを見よう．$x_1, x_2, \cdots, x_n$ を $\boldsymbol{R}^n$ の任意の正規直交基底とする．r_1 をつぎのように定める：

$$r_1 = \begin{cases} 1 & (f_A(x_1) = x_1 \text{ のとき}), \\ r_{y_1 - x_1} & (f_A(x_1) = y_1 \neq x_1 \text{ のとき}). \end{cases}$$

このとき $r_1 f_A = f_{A_1}$，$f_A(x_i) = x_i'$ とおくと，$f_{A_1}(x_1') = x_1'$ である．つぎに

$$r_2 = \begin{cases} 1 & (f_{A_1}(x_2') = x_2' \text{ のとき}), \\ r_{y_2 - x_2'} & (f_{A_1}(x_2') = y_2 \neq x_2' \text{ のとき}) \end{cases}$$

として，$f_{A_1}(x_i') = x_i''$，$f_{A_2} = r_2 f_{A_1}$ とおくと，$f_{A_2}(x_1'') = x_1''$，$f_{A_2}(x_2'') = x_2''$ である．この操作を n 回続けると，

$$f_{A_n} = r_n r_{n-1} \cdots r_1 f_A$$

が $\boldsymbol{R}^n$ の或る正規直交基底の各元を不変にするから，f_{A_n} は恒等変換となる．したがって

$$f_A = r_1 r_2 \cdots r_n \qquad (r_i^{-1} = r_i \text{ に注意}).$$

これは，R が $O(n)$ の生成系であることを示す．よりくわしく $O(n)$ の元は高々 n 個の鏡映の積として書けることがわかった．

問 1.39 上の (i), (ii) を証明せよ．またつぎの (iii), (iv), (v) を示せ：

(iii) $\det r_a = -1$. (iv) $A \in O(n)$ を鏡映の積として書いたとき，それが偶数個の積であるか奇数個の積であるかは A によって定まる．(v) $R' = \{r_a r_b \mid r_a, r_b \in R\}$ は $SO(n)$ の生成系である．

例 1.13 正2面体群 平面上の正 n 角形を自分自身に重ね合わす(空間における)回転の全体は群を作る．これは，

(α) 平面上の n 個の回転，

(β) n 本の対称軸のまわりの角 π の回転

からなる位数 $2n$ の群である．これを D_{2n} で表わし，位数 $2n$ の**正2面体群**という．a を平面上の角 $2\pi/n$ の回転，b を一つの対称軸のまわりの回転とすると，(α) に属するものは

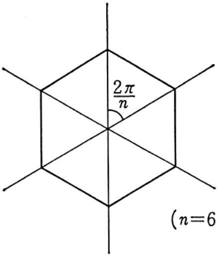
$$1, \ a, \ a^2, \ \cdots, \ a^{n-1}$$

であり，(β) に属するのは

$$b, \ ba, \ \cdots, \ ba^{n-1}$$

である．これから集合 $\{a, b\}$ は D_{2n} の生成系であることがわかる：

$$D_{2n} = \langle a, b \rangle.$$



(n=6) **図3**

ところで，D_{2n} の生成元 a, b はつぎの関係を満たす：

(1.15) $$a^n = 1, \quad b^2 = 1, \quad b^{-1}ab = a^{-1}.$$

問 1.40 (1.15) を確かめよ．——

D_{2n} の二つの元 $a^i b^j$, $a^k b^l$ ($0 \leqq i, k \leqq n-1$, $0 \leqq j, l \leqq 1$) の積は上の関係 (1.15) を

用いて計算することができる．たとえば

$$(ab)(a^2b) = a(ba)(ab) = a(a^{-1}b)ab = bab = a^{-1} = a^{n-1}$$

である．このように或る群の生成元の間の関係が群の演算を完全に決めてしまうとき(いいかえると群の構造を完全に決めてしまうとき)，その関係をその群の基本関係というのであるが，より正確にはつぎのように理解するべきである．

基本関係　一般に群 G が S で生成され，S の元は関係

(＊)　　$Q_\lambda(s_1, s_2, \cdots, s_n) = 1$　　($s_i \in S,\ \lambda \in \Lambda$＝添数集合)

を満たすとする．ここで $Q_\lambda(s_1, s_2, \cdots, s_n)$ は $s_1, s_2, \cdots, s_n$ のベキ積 ($s_1{}^{t_1}s_2{}^{t_2}\cdots s_n{}^{t_n}$ ($t_i \in \boldsymbol{Z}$) の形の G の元) である．つぎの‘**普遍性の条件**’が満たされるとき，関係(＊)を G の基本関係という：

G' をつぎの性質(i), (ii)を満たす任意の群とする．

(i) G' は S' で生成される，

(ii) S から S' への全射 $s \mapsto s'$ が存在して，S' は(＊)と同じ関係 $Q_\lambda(s_1', s_2', \cdots, s_n') = 1$ ($\lambda \in \Lambda$) を満たす．

このとき G から G' の上への準同型 f で $f(s) = s'$ なるものが存在する．——

簡単にいうと，S で生成される G が関係(＊)を持ったもっとも一般的な群であるとき，S の元の間の関係(＊)を G の基本関係というのである．定義からわかるように与えられた関係を基本関係とする群は(存在したとしても)同型を除いて一意的である．

注意　一般に**任意に**与えられた関係を基本関係とする群が存在することが証明される．しかしそれには自由群の概念が必要なので，それは第6章で述べられる．

正2面体群 D_{2n} の生成元 a, b を例1.13におけるようにとると，関係(1.15)は D_{2n} の基本関係である．実際 $G' = \langle a', b' \rangle$，$a'^n = 1$，$b'^2 = 1$，$b'^{-1}a'b' = a'^{-1}$ とすると，D_{2n} から G' の上への写像 $f: a^pb^q \mapsto a'^pb'^q$ ($p, q \in \boldsymbol{Z}$) は，$f(a) = a'$，$f(b) = b'$ なる D_{2n} から G' の上への準同型であることが直接の計算で確かめられる．しかしつぎの例の中で D_{2n} を含むより一般な群に対してこのことを示すであろう．

例 1.14　4元数型の群　二つの元 a, b で生成され，

(1.16)　　$b^2 = a^m, \quad a^{2m} = 1, \quad b^{-1}ab = a^{-1}$

を基本関係とする群を**4元数型の群**といい，Q_{4m} で表わす．とくに Q_8 ($m=2$) を**4元数群**とよぶ．Q_{4m} は位数 $4m$ の群である．以下このような群を構成し，そ

の位数が $4m$ であることを示そう.

注意　上の注意でも述べたように (1.16) を基本関係とする群の存在は一般論でも保証されている. また関係 (1.16) から Q_{4m} の位数が高々 $4m$ であることもほとんど明らかである. しかしながら, 実際に Q_{4m} の位数が $4m$ であることは ((1.16) から a の位数が $2m$ であることを示せばよいのだが), 決して明らかではない. このことを示そうとすると一般論にたよらずに存在証明をする (あるいはそれと同程度の議論をする) ことが必要である.

以下, Q_{4m}, D_{2n} を含むより一般的な群を構成しよう. $\boldsymbol{Z}^+=\{n\in\boldsymbol{Z}\mid n\geqq 0\}$, r を任意の整数として, $\boldsymbol{Z}\times\boldsymbol{Z}^+$ の上に

$$(i,j)(i',j')=(i+r^ji',j+j')\qquad ((i,j),(i',j')\in\boldsymbol{Z}\times\boldsymbol{Z}^+)$$

によって演算を定義すると, $\boldsymbol{Z}\times\boldsymbol{Z}^+$ は単位元 $(0,0)$ を持った半群となる. さらに m,n,k を整数でつぎの条件が満たされているものとする:

$$m>0,\qquad n>0,$$
$$rk\equiv k\pmod m,$$
$$r^n\equiv 1\pmod m.$$

このとき $\boldsymbol{Z}\times\boldsymbol{Z}^+$ の上の関係

$$(i,j)\sim(i',j')\iff j-j'\equiv 0\pmod n,\qquad k(j-j')/n+i-i'\equiv 0\pmod m$$

は, 補題1.2の条件を満たす半群 $\boldsymbol{Z}\times\boldsymbol{Z}^+$ の上の同値関係である. したがってこの同値関係による商集合は群となる. これを $\boldsymbol{Z}(m,n,r,k)$ と書くと, 明らかに

$$|\boldsymbol{Z}(m,n,r,k)|=mn$$

である. また $a=\overline{(1,0)}$ ($=(1,0)$ を含む同値類), $b=\overline{(0,1)}$ とおくと, a,b は関係

$$b^n=a^k,\qquad a^m=1,\qquad b^{-1}ab=a^r \tag{1.17}$$

を満たすことが直接の計算で確かめられる. このとき関係 (1.17) は $\boldsymbol{Z}(m,n,r,k)$ の基本関係であることがつぎのように示される. $G'=\langle a',b'\rangle$, $b'^n=a'^k$, $a'^m=1$, $b'^{-1}a'b'=a'^r$ とすると, $\boldsymbol{Z}\times\boldsymbol{Z}^+$ から G' の上への写像 f

$$f:\ (i,j)\longmapsto a'^ib'^j$$

は, 半群 $\boldsymbol{Z}\times\boldsymbol{Z}^+$ から G' の上への準同型

(i)　$f((i,j)(i',j'))=f((i,j))f((i',j'))$

であって, しかも

(ii)　$(i,j)\sim(i',j')\implies f((i,j))=f((i',j'))$

であることが容易に確かめられる. したがって f は自然に $\boldsymbol{Z}(m,n,r,k)$ から G'

の上への準同型 $\bar{f}$ で $\bar{f}(a)=a'$, $\bar{f}(b)=b'$ なるものをひき起す．すなわち関係(1.17)は $\boldsymbol{Z}(m,n,r,k)$ の基本関係である．

$m=2m'$, $n=2$, $k=m'$, $r=-1$ のときが最初に述べた4元数型の群である：$Q_{4m}=\boldsymbol{Z}(2m,2,-1,m)$．また $n=2$, $k=0$, $r=-1$ のときは，$D_{2m}=\boldsymbol{Z}(m,2,-1,0)$ となる．

問 1.41 上の(i), (ii)を確かめよ．

問 1.42 4元数型の群 Q_{4m} は位数2の部分群をただ一つ含むことを示せ．それを Z とすると，$Q_{4m}\triangleright Z$, $Q_{4m}/Z\simeq D_{2m}$ であることを示せ．

問 1.43 4元数群 Q_8 の部分群はすべて正規部分群であることを示せ．

問 1.44 G を有限群，N を G の正規部分群とする．N および G/N が巡回群ならば，或る m,n,r,k に対して $G\simeq\boldsymbol{Z}(m,n,r,k)$ であることを示せ．——

最後に G の生成系と部分群の生成系の関係を与える一つの補題を証明しよう．

補題 1.5 H を G の部分群，T を H の右剰余類の代表系で $T\ni 1$ とする．$G=\langle S\rangle$ ならば $H=\langle TST^{-1}\cap H\rangle$ である．とくに G が有限生成ならば G の指数有限の部分群も有限生成である．

証明 G の各元 x は，$x=ht$ $(h\in H,\ t\in T)$ と一意的に書き表わされる．このとき G から H への写像 η を

$$\eta:\ x\longmapsto h \qquad (x=ht,\ h\in H,\ t\in T)$$

によって定義する．この η を用いれば，

$$TST^{-1}\cap H=\{\eta(ts)\,|\,t\in T,\ s\in S\}$$

である．さて $\eta(s_1s_2\cdots s_n)$ $(s_i\in S\cup S^{-1})$ が

$$T(S\cup S^{-1})T^{-1}\cap H=(TST^{-1}\cap H)\cup(TST^{-1}\cap H)^{-1}$$

の元の積として書けることを n に関する数学的帰納法によって示そう．$n=1$ ならば，$T\ni 1$ により $\eta(s_1)=\eta(1s_1)\in TST^{-1}\cap H$ となる．$s_1s_2\cdots s_{n-1}=ht$ $(h\in H,\ t\in T)$ とおくと，$\eta(s_1s_2\cdots s_n)=\eta(hts_n)=h\eta(ts_n)$ である．$h=\eta(s_1s_2\cdots s_{n-1})$ は帰納法の仮定により $T(S\cup S^{-1})T^{-1}\cap H$ の元の積である．したがって $\eta(s_1s_2\cdots s_n)=\eta(s_1s_2\cdots s_{n-1})\eta(ts_n)$ もそうである．ところで $G\ni x$ ならば $x=s_1s_2\cdots s_n$ $(s_i\in S\cup S^{-1})$ であり，とくに $H\ni x$ ならば $x=\eta(x)=\eta(s_1s_2\cdots s_n)$ だから，H の各元は $T(S\cup S^{-1})T^{-1}\cap H$ の元の積である．これは $H=\langle TST^{-1}\cap H\rangle$ を示す．G が有限生成で H が指数有限ならば，T,S ともに有限集合であるから，$TST^{-1}\cap H$ も

有限集合である. ▌

問 1.45 $\mathfrak{S}_n$ の生成系 $(1\ 2), (2\ 3), \cdots, (n-1\ n)$ から補題1.5の方法で $\mathfrak{A}_n$ の生成系を作り, $\mathfrak{A}_n$ は $(1\ 2\ 3), (1\ 2)(3\ 4), (1\ 2)(4\ 5), \cdots, (1\ 2)(n-1\ n)$ で生成されることを示せ.

§1.6 共役類

a) 定義と例

$G \ni x, y$ に対して

$$zxz^{-1} = y \qquad (\exists z \in G)$$

なるとき, x と y は G で**共役**であるという. この関係は G の上の同値関係である. その同値類を**共役類**という. 共役類の概念は群論において重要である.

例 1.15 行列論によれば, n 次正方行列 A は, $P \in GL_n(\boldsymbol{C})$ を適当にとれば, $P^{-1}AP$ が Jordan の標準形

$$P^{-1}AP = \begin{bmatrix} J(\alpha_1, k_1) & & & \\ & J(\alpha_2, k_2) & & \\ & & \ddots & \\ & & & J(\alpha_r, k_r) \end{bmatrix} \qquad (\alpha_i \in \boldsymbol{C}),$$

$$J(\alpha, k) = \left.\begin{bmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \alpha \end{bmatrix}\right\} k$$

となる. ここで, $J(\alpha_1, k_1)$, $J(\alpha_2, k_2)$, $\cdots$, $J(\alpha_r, k_r)$ は (並べる順序を無視すれば) A に対して一意的に定まる (§3.5 例題3.3参照). このことは, 一般線型群 $GL_n(\boldsymbol{C})$ の共役類の代表系として Jordan の標準形がとれることを示している. またユニタリ群 $U(n)$ の共役類の代表系としては, 絶対値1の複素数を対角成分とする対角行列がとれる. これも行列論でよく知られた "正規行列 A は適当にユニタリ行列 U をとって $U^{-1}AU = U^*AU$ が対角行列となる" という命題の特別の場合である. 実直交群 $O(n)$ の共役類の代表系としては, n が偶数のとき

$$\pm\begin{bmatrix} R(\theta_1) & & & \\ & R(\theta_2) & & \\ & & \ddots & \\ & & & R(\theta_{n/2}) \end{bmatrix} \quad (\pi \geqq \theta_i \geqq 0),$$

n が奇数のとき

$$\begin{bmatrix} R(\theta_1) & & & & \\ & R(\theta_2) & & & \\ & & \ddots & & \\ & & & R(\theta_{(n-1)/2}) & \\ & & & & \pm 1 \end{bmatrix} \quad (\pi \geqq \theta_i \geqq 0)$$

がとれる．ここで

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

である．これからとくに $n=3$ のとき，$SO(3)$ の共役類の代表系として

$$\begin{bmatrix} \cos\theta & -\sin\theta & \\ \sin\theta & \cos\theta & \\ & & 1 \end{bmatrix} \quad (\pi \geqq \theta \geqq 0)$$

がとれることがわかる．これを，幾何学的にいえば，x, y, z 軸を適当にとったとき，z 軸のまわりの角 $\theta\,(0 \leqq \theta \leqq \pi)$ の回転を表わすから，$SO(3)$ の二つの元は回転の角が等しいときそのときに限り共役である．(回転角 θ が $\pi < \theta \leqq 2\pi$ のときは x, y, z 軸の向きを適当に変えれば，π 以下の回転となることに注意.)

問 1.46 n が奇数のとき，$SO(n)$ の二つの元が共役であるためにはそれらが $O(n)$ で共役であることが必要十分である．n が偶数のときは，このことは成り立たないことも確かめよ．——

x を含む共役類を C_x，x の中心化群 $C_G(x) = \{y \in G \mid xy = yx\}$ を H とすると，C_x と H の左剰余類の集合 G/H の間には

$$zxz^{-1} \longleftrightarrow zH \qquad (z \in G)$$

なる 1 対 1 の対応がある(問 1.18 参照)．とくに G が有限群のときにはつぎの定理が成り立つ．

定理 1.7 G を有限群とする．$G \ni x$ を含む共役類は $[G : C_G(x)]$ 個の元からなる．とくに各共役類に含まれる元の数は G の位数の約数である．——

有限群 G のすべての共役類を $C_1, C_2, \cdots, C_q$ とし，C_i に含まれる元の数を l_i とすれば，

$$|G| = l_1+l_2+\cdots+l_q, \qquad l_i \mid |G|$$

である．これを有限群 G の**類等式**という．単位元を含む共役類は明らかに単位元のみからなるから，$l_1, l_2, \cdots, l_q$ のうち少なくとも一つは1である．群 G の中心 $Z(G)$：

$$Z(G) = \{x \in G \mid xy=yx \ (\forall y \in G)\}$$

の各元は，それだけで一つの共役類を作る：

$$Z(G) \ni x \iff x \text{ を含む共役類は } x \text{ のみからなる.}$$

有限群 G の類等式において $l_i=1$ なる項をまとめて

$$|G| = z+l_1+\cdots+l_q, \qquad z = |Z(G)|, \qquad 1 < l_i \mid |G|$$

と書き，これを G の類等式ということもある．

例 1.16 (対称群の共役類)　対称群の共役類を記述するにはつぎのことが基本になる：

> 任意の置換は共通の文字を含まない巡回置換の積として(積の順序を無視すれば)一意的に書ける．

以下では置換 σ を巡回置換の積として表示するとき，σ によって不変な文字を長さ1の巡回置換として明示することにする．たとえば

$$\mathfrak{S}_7 \ni \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 4 & 6 & 5 & 3 \end{pmatrix} = (1)(4)(2\ 7\ 3)(5\ 6)$$

である．さて n 次対称群 $\mathfrak{S}_n$ の元 σ が，長さ1の巡回置換 a_1 個，長さ2の巡回置換 a_2 個，…，長さ n の巡回置換 a_n 個の積として書けるとき，σ は $1^{a_1}2^{a_2}\cdots n^{a_n}$ 型であるという．上の例は，$1^2 2^1 3^1 4^0 5^0 6^0 7^0$ 型の元である．$a_1, a_2, \cdots, a_n$ の間には明らかに

$$a_1+2a_2+\cdots+na_n = n \qquad (a_i \geqq 0) \tag{1.18}$$

なる関係がある．

定理 1.8　$\mathfrak{S}_n$ の2元が共役であるためには，この2元の型が同じであることが必要十分である．

証明　$\mathfrak{S}_n \ni \sigma$ を $1^{a_1}2^{a_2}\cdots n^{a_n}$ 型としよう：

$$\sigma = \underbrace{(i_1)(i_2)\cdots(i_{a_1})}_{a_1}\underbrace{(j_1\ j_{1'})\cdots(j_{a_2}\ j_{a_2'})}_{a_2}\cdots.$$

$\tau=\begin{pmatrix} i_1 & i_2 & \cdots & i_{a_1} & j_1 & j_{1'} & \cdots & j_{a_2} & j_{a_2'} & \cdots \\ i_1' & i_2' & \cdots & i_{a_1}' & j_1' & j_{1'}' & \cdots & j_{a_2}' & j_{a_2'}' & \cdots \end{pmatrix}$ とすると,

$$\tau\sigma\tau^{-1} = (i_1')(i_2')\cdots(i_{a_1}')(j_1'\ j_{1'}')\cdots(j_{a_2}'\ j_{a_2'}')\cdots$$

となり, $\tau\sigma\tau^{-1}$ も $1^{a_1}2^{a_2}\cdots n^{a_n}$ 型である. 逆に σ と σ' が同じ型のとき, $\tau\sigma\tau^{-1}=\sigma'$ なる τ の作り方もこのことから明らかであろう. ▌

p_n を n を正整数の和として書く書き表わし方の数(和の順序は無視する)とすれば, (1.18) と定理 1.8 から n 次対称群 $\mathfrak{S}_n$ の共役類の数は p_n に等しいことがわかる. たとえば, $n=3$ とすれば

$$3 = 1+1+1, \quad 3 = 1+2, \quad 3 = 3$$

であるから, 3 次対称群は三つの共役類をもち

$$\text{単位元} = 1^3 2^0 3^0\ 型, \quad (1\ 2) = 1^1 2^1 3^0\ 型, \quad (1\ 2\ 3) = 1^0 2^0 3^1\ 型$$

が各共役類の代表元である.

問 1.47 $\mathfrak{S}_4, \mathfrak{S}_5$ の共役類の代表元を求めよ.

問 1.48 $1^{a_1}2^{a_2}\cdots n^{a_n}$ 型の共役類の元の数は

$$\frac{n!}{1^{a_1}a_1!2^{a_2}a_2!\cdots n^{a_n}a_n!} = \frac{n!}{\prod_{i=1}^{n} i^{a_i}a_i!}$$

であることを示せ. また $\mathfrak{S}_n$ $(n\geqq 3)$ の中心は単位元のみからなることを示せ.

問 1.49 正 2 面体群 D_{2n}, 4 元数型の群 Q_{4m} の共役類と類等式を求めよ.

問 1.50 G の部分群 H が正規部分群であるためには, H が G のいくつかの共役類の和集合であることが必要十分であることを示せ. またこのことに注意してつぎのことを示せ: $\mathfrak{A}_4, \mathfrak{A}_5$ の類等式を作り, これを用いて $\mathfrak{A}_4$ は指数 2 の部分群をもたないこと, $\mathfrak{A}_5$ の正規部分群は自明なものに限ること.

b) n 次交代群 $\mathfrak{A}_n$ $(n\geqq 5)$ の単純性

一般に群 G の正規部分群が自明なもの (G 自身および単位群) に限るとき, G を**単純群**という. 素数位数の有限群は明らかに単純群である.

問 1.51 可換な単純群は素数位数であることを示せ. ——

問 1.50 によれば, 5 次交代群は非可換単純群である. このほかにも応用上大切な群の中に多くの非可換単純群の例がある. 本書でも第 2 章でそのような例を

見るが，ここでは n 次交代群 $\mathfrak{A}_n\,(n\geqq 5)$ の単純性の一つの証明を与えよう．

定理 1.9　$n\geqq 5$ のとき，n 次交代群 $\mathfrak{A}_n$ は非可換単純群である．

証明　(α)　長さ3のすべての巡回置換の集合は，$\mathfrak{A}_n$ の一つの共役類である．

実際，$(1\ 2\ 3)$, $(i\ j\ k)$ $(i\neq j\neq k\neq i)$ に対して $\tau(1\ 2\ 3)\tau^{-1}=(i\ j\ k)$ なる偶置換の存在を示せばよいが，定理1.8によりこのような $\mathfrak{S}_n$ の元 τ がとれる．τ が奇置換のときは，$\tau'=\tau(4\ 5)$ とおくと τ' は偶置換で $\tau'(1\ 2\ 3)\tau'^{-1}=(i\ j\ k)$ となる．

(β)　$\mathfrak{A}_n\triangleright N\neq 1$ のとき，N は長さ3の巡回置換を含む．

N の元 $\sigma\neq 1$ で σ によって不変な文字の数が最大になるようなものを考える．このような σ が長さ3の巡回置換であることを示そう．背理法で証明することにして σ によって動かされる文字の数が4以上であるとしてみよう．このとき σ を共通の文字を含まない巡回置換の積として書いてつぎの二つの場合に分ける：

(i)　σ は互換の積である場合，

(ii)　σ は長さ3以上の巡回置換を少なくとも一つ含む場合．

(i) の場合：$\sigma=(1\ 2)(3\ 4)\cdots$ としてよい．このとき σ によって不変な5以下の文字は高々一つである．σ の $\tau=(3\ 4\ 5)$ による共役 $\sigma'=\tau\sigma\tau^{-1}$ を作れば $N\ni\sigma'=(1\ 2)(4\ 5)\cdots$ となり $1\neq\sigma^{-1}\sigma'\in N$ である．5より大きい文字 a が σ によって不変ならば a は $\sigma^{-1}\sigma'$ によっても不変である．実際 $\tau(a)=a$ により，$\sigma^{-1}\sigma'(a)=\sigma^{-1}\tau\sigma\tau^{-1}(a)=\sigma^{-1}\tau\sigma(a)=\sigma^{-1}\tau(a)=\sigma^{-1}(a)=a$ となる．また $\sigma^{-1}\sigma'(1)=1$, $\sigma^{-1}\sigma'(2)=2$ であるから，$\sigma^{-1}\sigma'$ によって不変な文字の数は σ によるそれよりも多くなり σ のとり方に反する．

(ii) の場合：$\sigma=(1\ 2\ 3\ \cdots)\cdots$ としてよい．このとき σ は少なくとも五つの文字を動かす．実際 σ がちょうど四つの文字を動かせば σ は長さ4の巡回置換となり，これは奇置換だから矛盾である．したがって σ は文字 $1, 2, 3, 4, 5$ を実際に動かすとしてよい．(i) の場合と同様に σ の $\tau=(3\ 4\ 5)$ による共役 $\sigma'=\tau\sigma\tau^{-1}$ を作れば $\sigma'=(1\ 2\ 4\ \cdots)\cdots$ となる．$a>5$ が σ によって不変ならば $\sigma^{-1}\sigma'$ によっても不変であり，さらに $\sigma^{-1}\sigma'(1)=1$ であるから，この場合も N の元 $\sigma^{-1}\sigma'$ によって不変な文字の数は σ によるそれよりも多くなり σ のとり方に反する．

(γ)　$\mathfrak{A}_n\triangleright N\neq 1$ ならば，$\mathfrak{A}_n=N$．すなわち $\mathfrak{A}_n\,(n\geqq 5)$ は単純群である．

長さ3の巡回置換全体を C としよう．(β) により $N\cap C\neq\phi$．$\mathfrak{A}_n\triangleright N$ および

(α)により $N \supseteq C$(問1.50により N は $\mathfrak{A}_n$ の共役類の和集合であることに注意). ところで例1.10により C は $\mathfrak{A}_n$ の生成系であるから, $\mathfrak{A}_n = \langle C \rangle$. したがって $\mathfrak{A}_n = N$ でなければならない. ▌

上で示した $\mathfrak{A}_n$ ($n \geqq 5$) の単純性は方程式論への重要な応用を持つ. すなわち有名な Abel の定理“5次以上の代数方程式は, 一般には代数的には解けない”の群論的根拠を与えるのが, $\mathfrak{A}_n$ ($n \geqq 5$) の単純性である. これについては本選書の“体と Galois 理論”を参照されたい.

§1.7 環 と 体

集合 $\mathfrak{R}$ に和と積で表わされる二つの演算

$$\mathfrak{R} \times \mathfrak{R} \ni (x, y) \longmapsto x+y \in \mathfrak{R},$$

$$\mathfrak{R} \times \mathfrak{R} \ni (x, y) \longmapsto xy \in \mathfrak{R}$$

が定義されていて, つぎの公理を満たすとき $\mathfrak{R}$ を**環**という:

I　$\mathfrak{R}$ は加法に関して加群である,

II　$\mathfrak{R}$ は乗法に関して単位元1をもった半群である,

III　分配法則

$$x(y+z) = xy+xz, \qquad (x+y)z = xz+yz \qquad (x, y, z \in \mathfrak{R})$$

が成り立つ.

環 $\mathfrak{R}$ の部分集合 $\mathfrak{R}'$ が

(α)　$a, b \in \mathfrak{R}' \Longrightarrow a \pm b \in \mathfrak{R}',\ ab \in \mathfrak{R}'$,

(β)　$1 \in \mathfrak{R}'$

を満たすとき, $\mathfrak{R}'$ を $\mathfrak{R}$ の**部分環**という.

注意　環の定義において, 乗法に関する単位元の存在を要請しないこともある. また部分環の定義でも(たとえ $\mathfrak{R}$ が乗法の単位元を持っていても)条件(β)を仮定しないことがある. しかし本書ではつねに上の定義にしたがうであろう.

公理 I, II, III に加えて

II′　$xy = yx \quad (\forall x, y \in \mathfrak{R})$

が成り立つとき, $\mathfrak{R}$ を**可換環**という. 整数の集合 $\boldsymbol{Z}$, 複素数の集合 $\boldsymbol{C}$ は, 数の通常の加法, 乗法に関して可換環である. また n 次複素行列の集合 $M_n(\boldsymbol{C})$ は行列の加法, 乗法に関して環($n>1$ ならば非可換な環)である. より一般に環 $\mathfrak{R}$ の

元を成分とする n 次正方行列全体の集合 $M_n(\mathfrak{R})$ は，行列の加法と乗法を $M_n(\boldsymbol{C})$ におけるのとまったく同様に定義すれば，環となる．$M_n(\mathfrak{R})$ を $\mathfrak{R}$ 上の **n 次行列環**という．

環 $\mathfrak{R}$ はつぎの条件を満たすとき，**斜体**とよばれる：

II″　$\mathfrak{R}^\sharp=\mathfrak{R}-\{0\}$ は乗法に関して群である．

とくに $\mathfrak{R}^\sharp$ が Abel 群のとき $\mathfrak{R}$ を**可換体**あるいは簡単に**体**という．有理数の集合 $\boldsymbol{Q}$，実数の集合 $\boldsymbol{R}$，複素数の集合 $\boldsymbol{C}$ などは体である．可換体でない斜体としてもっとも有名なのは Hamilton の 4 元数体である．$\boldsymbol{H}$ をつぎの形の 2 次複素行列の集合とする：

$$\boldsymbol{H}=\left\{\begin{bmatrix}\alpha & -\beta\\ \bar{\beta} & \bar{\alpha}\end{bmatrix}\middle|\,\alpha,\beta\in\boldsymbol{C}\right\}\qquad(\bar{\ }\text{ は複素共役を表わす}).$$

このとき $\boldsymbol{H}$ は行列の加法，乗法に関して(非可換な)斜体となることが容易に確かめられる．$\boldsymbol{H}$ を **Hamilton の 4 元数体**という．

$$1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad i=\begin{bmatrix}\sqrt{-1} & 0\\ 0 & -\sqrt{-1}\end{bmatrix},\quad j=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\quad k=\begin{bmatrix}0 & -\sqrt{-1}\\ -\sqrt{-1} & 0\end{bmatrix}$$

とおくと，

$$i^2=j^2=k^2=-1,\quad k=ij=-ji,\quad j=ki=-ik,\quad i=jk=-kj$$

であり，$\boldsymbol{H}$ の元は

$$a+bi+cj+dk\qquad(a,b,c,d\in\boldsymbol{R})$$

の形に一意的に書ける．

問 1.52　$\{\pm1,\pm i,\pm j,\pm k\}$ は $\boldsymbol{H}$ における乗法に関して群であることを示せ．またこの群は 4 元数群 Q_8 と同型である．

問 1.53　$G=\{a+bi+cj+dk\in\boldsymbol{H}\,|\,a^2+b^2+c^2+d^2=1\}$ は $\boldsymbol{H}^\sharp=\boldsymbol{H}-\{0\}$ の部分群で，$G\simeq SU(2)$ (2 次元特殊ユニタリ群) であることを示せ．

例 1.17 (群環)　G を有限群，$\mathfrak{R}$ を可換環とする．$\mathfrak{R}$ の元を係数とするつぎのような形式和

$$\sum_{x\in G}r_x x\qquad(r_x\in\mathfrak{R})$$

の集合を $\mathfrak{R}[G]$ と書く．$\mathfrak{R}[G]$ につぎのように自然に和と積を定義する：

$$\sum_{x\in G}r_x x+\sum_{x\in G}s_x x=\sum_{x\in G}(r_x+s_x)x,$$

$$\left(\sum_x r_x x\right)\left(\sum_x s_x x\right) = \sum_x t_x x, \qquad t_x = \sum_{y\in G} r_y s_{y^{-1}x} \in \mathfrak{R}.$$

このとき $\mathfrak{R}[G]$ は環となることが容易に確かめられる．このような環を有限群 G の $\mathfrak{R}$ 上の**群環**という．

環 $\mathfrak{R}$ の部分集合 $\mathfrak{A}$ は

(α) $a, b \in \mathfrak{A} \Longrightarrow a+b \in \mathfrak{A}$, $-a \in \mathfrak{A}$,

(β) $a \in \mathfrak{A}$, $c \in \mathfrak{R} \Longrightarrow ca \in \mathfrak{A}$

なる条件を満たすとき，**左イデアル**とよばれる．(β) の代りに

(β)′ $a \in \mathfrak{A}$, $c \in \mathfrak{R} \Longrightarrow ac \in \mathfrak{A}$

を満たすとき $\mathfrak{A}$ を**右イデアル**という．$\mathfrak{A}$ が (α), (β), (β)′ を満たすとき，すなわち $\mathfrak{A}$ が左イデアルでも右イデアルでもあるとき，**両側イデアル**あるいは単に**イデアル**とよばれる．可換環 $\mathfrak{R}$ においては，明らかに右イデアル，左イデアル，両側イデアルの概念はすべて一致し区別する必要はない．

可換環 $\mathfrak{R}$ の元 a に対して

$$\langle a\rangle = \{xa \mid x \in \mathfrak{R}\}$$

とおくと，$\langle a\rangle$ は $\mathfrak{R}$ のイデアルである．このようなイデアルを a によって生成される**主イデアル**という．より一般に $\mathfrak{R} \ni a_1, a_2, \cdots, a_n$ に対して

$$\langle a_1, a_2, \cdots, a_n\rangle = \{x_1a_1+x_2a_2+\cdots+x_na_n \mid x_i \in \mathfrak{R}\}$$

はイデアルであり，このようなイデアルを $a_1, a_2, \cdots, a_n$ によって生成されるイデアルという．

問 1.54 整数環 $\boldsymbol{Z}$ のイデアルはすべて主イデアルであることを示せ．

問 1.55 斜体 k 上の n 次行列環 $M_n(k)$ に対してつぎのことを示せ．

(i) 或る列以外の成分がすべて 0 である行列全体は左イデアルである．

(ii) 或る行以外の成分がすべて 0 である行列全体は右イデアルである．

(iii) 両側イデアルは自明なもの ($M_n(k)$ および $\{0\}$) に限る．

問 1.56 G を有限群，$\mathfrak{R}$ を可換環とする．群環 $\mathfrak{R}[G]$ の部分集合 $\left\{r\sum_{x\in G} x \mid r \in \mathfrak{R}\right\}$, $\left\{\sum_{x\in G} r_x x \mid \sum_{x\in G} r_x = 0\right\}$ は $\mathfrak{R}[G]$ のイデアルであることを示せ．——

$\mathfrak{A}$ が環 $\mathfrak{R}$ のイデアルであるとき，$\mathfrak{R} \ni x, y$ に対して

$$x \equiv y \pmod{\mathfrak{A}} \quad \text{すなわち} \quad x-y \in \mathfrak{A}$$

なる関係は $\mathfrak{R}$ 上の同値関係であり，その商集合 $\bar{\mathfrak{R}}$ の上に和と積を自然に定義す

ると $\bar{\mathfrak{R}}$ は環となる．このようにして構成された環 $\bar{\mathfrak{R}}$ を $\mathfrak{R}$ の $\mathfrak{A}$ による**剰余環**といい，$\mathfrak{R}/\mathfrak{A}$ で表わされる．

$\mathfrak{R}, \mathfrak{R}'$ を環，f を $\mathfrak{R}$ から $\mathfrak{R}'$ への写像とする．f がつぎの条件

(α)　$f(x+y) = f(x)+f(y) \quad (x, y \in \mathfrak{R})$,

(β)　$f(xy) = f(x)f(y)$,

(γ)　$f(1) = 1'$　($1, 1'$ はそれぞれ $\mathfrak{R}, \mathfrak{R}'$ の乗法の単位元)

を満たすとき，f を $\mathfrak{R}$ から $\mathfrak{R}'$ への**準同型**(写像)という．とくに f が全単射のとき，f を $\mathfrak{R}$ から $\mathfrak{R}'$ の上への**同型**(写像)という．$\mathfrak{R}$ から $\mathfrak{R}'$ の上への同型が存在するとき $\mathfrak{R}$ と $\mathfrak{R}'$ は**同型**であるといい，

$$\mathfrak{R} \simeq \mathfrak{R}'$$

と書く．

問 1.57 (準同型定理)　f を $\mathfrak{R}$ から $\mathfrak{R}'$ の上への準同型とする．つぎのことを示せ：(i) $f^{-1}(0')$ ($0'$ は $\mathfrak{R}'$ の零元) は $\mathfrak{R}$ のイデアルである．(ii) $\mathfrak{R}/f^{-1}(0') \simeq \mathfrak{R}'$. ——

環 $\mathfrak{R}$ に対して

$$\mathfrak{R}_0 = \{m \cdot 1 \mid m \in \boldsymbol{Z}\} \qquad (1 \text{ は } \mathfrak{R} \text{ の乗法の単位元})$$

とおく．$\mathfrak{R}_0$ は $\mathfrak{R}$ の部分環であり，$\boldsymbol{Z}$ から $\mathfrak{R}_0$ の上への写像

$$\boldsymbol{Z} \ni m \longmapsto m \cdot 1 \in \mathfrak{R}_0$$

は $\boldsymbol{Z}$ から $\mathfrak{R}_0$ の上への準同型である．その核を $\langle n \rangle$ $(0 \leqq n \in \boldsymbol{Z})$ とすると準同型定理(問 1.57)により

$$\boldsymbol{Z}/\langle n \rangle \simeq \mathfrak{R}_0$$

である．このとき n を $\mathfrak{R}$ の**標数**という．

環 $\mathfrak{R}$ の元 a に対して

$$aa' = a'a = 1$$

を満たす a' が存在するとき，a を $\mathfrak{R}$ の**単元**あるいは**正則元**，a' を a の逆元といい，$a' = a^{-1}$ と書く．$\mathfrak{R}$ の単元全体の集合は $\mathfrak{R}$ の乗法に関して群を作る．これを $\mathfrak{R}$ の**乗法群**といい，$\mathfrak{R}^*$ で表わす．$\boldsymbol{Z}$ の単元は ± 1 であり，したがって $\boldsymbol{Z}$ の乗法群 $\boldsymbol{Z}^*$ は位数 2 の群である．$\mathfrak{R}$ が斜体のときは，$\mathfrak{R}^*$ は 0 でない $\mathfrak{R}$ の元全体の集合にほかならない．

例 1.18　$\boldsymbol{Z} \ni n > 0$ とする．$\boldsymbol{Z}$ の主イデアル $\langle n \rangle$ による剰余環を $\boldsymbol{Z}_n$ と書く．

$\boldsymbol{Z}_n$ は n 個の元からなる可換環である．$\boldsymbol{Z}_n$ は加法に関して位数 n の巡回群である．また $\boldsymbol{Z}_n$ の乗法群 $\boldsymbol{Z}_n{}^*$ は例 1.5 で構成された位数 $\varphi(n)$ の Abel 群にほかならない．とくに $\boldsymbol{Z}_n$ が体であるためには，n が素数であることが必要十分である．したがって斜体の標数は 0 または素数である．

問 1.58 Gauss の整数環 $\boldsymbol{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\boldsymbol{Z}\}$ の乗法群を求めよ．$\boldsymbol{H_Z}=\{a+bi+cj+dk\mid a,b,c,d\in\boldsymbol{Z}\}$ は Hamilton の 4 元数体の部分環である．$\boldsymbol{H_Z}$ の乗法群を求めよ．——

可換環 $\mathfrak{R}$ の元を成分とする n 次行列に対してその行列式が通常の場合と同じように定義される．すなわち $M_n(\mathfrak{R})\ni A=(a_{ij})$ に対して

$$\det A=\sum_{\sigma\in\mathfrak{S}_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

と定義するのである．このとき行列式の周知の性質——多重線型性，交代性，$\det A=\det{}^tA$，$\det AB=\det A\det B$——が成り立つ．つぎの補題は，これもまた行列式のよく知られた性質であるが，便利なので本書でもときどき用いられる．

補題 1.6 A, B を $\mathfrak{R}$ の元を成分とする行列で，A は m 行 n 列，B は n 行 m 列の行列とする．このとき

$$\det AB=\begin{cases}0 & (m>n \text{ のとき}),\\ \displaystyle\sum_{i_1<i_2<\cdots<i_m}\det A(i_1i_2\cdots i_m)\det B(i_1i_2\cdots i_m) & (m\leqq n \text{ のとき}).\end{cases}$$

ここで $A(i_1i_2\cdots i_m)$ は A から第 $i_1,i_2,\cdots,i_m$ 列をとりだして作った m 次行列，$B(i_1i_2\cdots i_m)$ は B から第 $i_1,i_2,\cdots,i_m$ 行をとりだして作った m 次行列とする．——

環 $\mathfrak{R}$ 上の n 次行列環 $M_n(\mathfrak{R})$ の乗法群を $GL_n(\mathfrak{R})$ と書き，$\mathfrak{R}$ 上の **n 次一般線型群**という．$\mathfrak{R}$ が可換環ならば，$GL_n(\mathfrak{R})$ は行列式が $\mathfrak{R}$ の単元である n 次行列全体の集合にほかならない．また行列式が 1 の $M_n(\mathfrak{R})$ の元全体の集合を $SL_n(\mathfrak{R})$ と書けば，$SL_n(\mathfrak{R})$ は $GL_n(\mathfrak{R})$ の部分群である．$SL_n(\mathfrak{R})$ を $\mathfrak{R}$ 上の **n 次特殊線型群**という．

問 1.59 $\mathfrak{R}_1,\mathfrak{R}_2,\cdots,\mathfrak{R}_s$ を環，$\mathfrak{R}$ をこれらの直積集合とする：$\mathfrak{R}=\mathfrak{R}_1\times\mathfrak{R}_2\times\cdots\times\mathfrak{R}_s$．$\mathfrak{R}$ の上に自然に和と積を定義すると，$\mathfrak{R}$ は環となる．このとき，

$$GL_n(\mathfrak{R})\simeq GL_n(\mathfrak{R}_1)\otimes\cdots\otimes GL_n(\mathfrak{R}_s),$$

$$SL_n(\mathfrak{R})\simeq SL_n(\mathfrak{R}_1)\otimes\cdots\otimes SL_n(\mathfrak{R}_s).$$

ただし後者では $\mathfrak{R}_i$ $(1\leqq i\leqq s)$ は可換環とする．

問 1.60 $m=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ を整数 m の素因子分解とする．このとき

$$\boldsymbol{Z}_m \simeq \boldsymbol{Z}_{q_1}\times\cdots\times\boldsymbol{Z}_{q_r} \quad (\text{環としての同型}),$$
$$GL_n(\boldsymbol{Z}_m) \simeq GL_n(\boldsymbol{Z}_{q_1})\otimes\cdots\otimes GL_n(\boldsymbol{Z}_{q_r}) \qquad (q_i=p_i^{e_i}),$$
$$SL_n(\boldsymbol{Z}_m) \simeq SL_n(\boldsymbol{Z}_{q_1})\otimes\cdots\otimes SL_n(\boldsymbol{Z}_{q_r}).$$
——

体上の多項式環

k を体とする．X を一つの不定元としてつぎの形の式

$$a_0+a_1X+\cdots+a_nX^n \qquad (a_i\in k)$$

を k 上の**多項式**という．$n=0$ のときこれは k の元を表わす．$a_n\neq 0$ のとき，n をこの多項式の**次数**といい，$\deg f$ $(f(X)=a_0+a_1X+\cdots+a_nX^n)$ で表わす．k の元は次数 0 であるが便宜上 k の零元 0 に対しては $\deg 0=-\infty$ とおく．k 上の多項式全体の集合を $k[X]$ で表わせば，$k[X]$ に通常のように和と積を定義すると $k[X]$ は可換環となる：

$$\sum_\nu a_\nu X^\nu+\sum_\nu b_\nu X^\nu = \sum_\nu (a_\nu+b_\nu)X^\nu,$$
$$(\sum_\nu a_\nu X^\nu)(\sum_\nu b_\nu X^\nu) = \sum_\nu c_\nu X^\nu, \qquad c_\nu = \sum_{\mu+\lambda=\nu} a_\mu b_\lambda.$$

$k[X]$ を k 上の**多項式環**という．$k[X]\ni f(X)=a_0+a_1X+\cdots+a_nX^n$, $k\ni\alpha$ に対して

$$f(\alpha) = a_0+a_1\alpha+\cdots+a_n\alpha^n$$

とおく．$f(\alpha)=0$ のとき，α を $f(X)$ の**根**という．つぎの補題の証明は容易である．

補題 1.7 $k[X]\ni f, g,\ g\neq 0$ とする．このとき

$$f = qg+r, \qquad \deg r < \deg g$$

なる $q, r\in k[X]$ が存在して一意的である．

補題 1.8 (因数定理) $f(X)\in k[X]$ とする．

$$f(\alpha)=0 \quad (\alpha\in k) \Leftrightarrow f(X)=(X-\alpha)q(X) \quad (\exists q(X)\in k[X]).$$

補題 1.9 $k[X]\ni f(X)$, $\deg f=n$ のとき，$f(X)=0$ は k において高々 n 個しか根をもたない．

問 1.61 補題 1.7, 1.8, 1.9 を証明せよ．

問 1.62 体 k 上の多項式環のイデアルは，すべて主イデアルである．

定理 1.10 体の乗法群の有限部分群は巡回群である．

証明　k を体，G を k^* の有限部分群とする．補題 1.9 により任意の正整数 d に対し $X^d-1=0$ は k において高々 d 個しか根がない．とくに $X^d=1$ を満たす G の元の数は高々 d である．例題 1.4 により G は巡回群でなければならない．▌

定理 1.10 により有限体(有限個の元からなる体)の乗法群は巡回群である．とくに $\boldsymbol{Z}_p{}^*$ (p は素数)は位数 $p-1$ の巡回群である．

斜体上の線型空間

k を任意の斜体とする．集合 V が k 上の**線型空間**とは，

I　V は加群である，

II　$k\times V$ から V への写像

$$(\alpha, v)\longmapsto \alpha v$$

が与えられていて

$$\begin{aligned}(\alpha\beta)v &= \alpha(\beta v),\\ 1v &= v\end{aligned}\qquad (\alpha, \beta\in k,\ \ v\in V,\ \ 1 \text{ は } k \text{ の単位元}),$$

III　$$\begin{aligned}(\alpha+\beta)v &= \alpha v+\beta v,\\ \alpha(u+v) &= \alpha u+\alpha v\end{aligned}\qquad (\alpha, \beta\in k,\ \ u, v\in V)$$

なる条件を満たすもののことである．V の元をベクトルとよぶことがある．V の部分集合 U が

$$u, v\in U,\quad \alpha, \beta\in k \Longrightarrow \alpha u+\beta v\in U$$

なる条件を満たすとき，U を V の**部分空間**という．U は自然に k 上の線型空間となる．$V\ni v_1, v_2, \cdots, v_n$ が

$$\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_nv_n = 0 \Longrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

(ここで左辺の 0 は加群 V の零元，右辺の 0 は k の零元)であるとき，$v_1, v_2, \cdots, v_n$ は k 上**線型独立**であるという．線型独立でないとき，k 上**線型従属**という．

V の部分集合 S に対して，

$$\{\alpha_1v_1+\alpha_2v_2+\cdots+\alpha_nv_n \,|\, \alpha_i\in k,\ v_i\in S\}$$

は，V の部分空間である．これを S で生成される V の部分空間といい，$\langle S\rangle$ で表わす．とくに $V=\langle S\rangle$ のとき S を V の**生成系**という．V が有限集合 S で生成されるとき V は**有限生成**であるという．

$\{u_1, u_2, \cdots, u_r\}$，$\{v_1, v_2, \cdots, v_s\}$ は k 上線型独立なベクトルの二つの集合で

$$\langle u_1, u_2, \cdots, u_r\rangle = \langle v_1, v_2, \cdots, v_s\rangle$$

を満たすとき,

$$\{u_1, u_2, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\}$$

と書く. これは, V の線型独立な有限個のベクトルの集合 $\{u_1, u_2, \cdots, u_r\}$ 全体の集合の上の同値関係である.

(α) $\{u_1, u_2, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\} \Longrightarrow r = s$.

[証明] まず u_1 を適当な v_{i_1} でおきかえて

$$\{v_{i_1}, u_2, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\}$$

となることを示す. $u_1, u_2, \cdots, u_r$ の線型独立性により $\{u_1, u_2, \cdots, u_r\} \not\sim \{u_2, u_3, \cdots, u_r\}$ であるから, $\{u_2, u_3, \cdots, u_r\} \not\sim \{v_1, v_2, \cdots, v_s\}$. よって $v_{i_1} \notin \langle u_2, \cdots, u_r\rangle$ なる v_{i_1} が存在する. このとき明らかに $v_{i_1}, u_2, \cdots, u_r$ は線型独立かつ $\langle v_{i_1}, u_2, \cdots, u_r\rangle \subseteqq \langle u_1, u_2, \cdots, u_r\rangle$ である. ところが $v_{i_1} \in \langle u_1, u_2, \cdots, u_r\rangle$ より

$$v_{i_1} = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_r u_r$$

と書くと $\alpha_1 \neq 0$, よって

$$u_1 = \alpha_1^{-1} v_{i_1} - \alpha_1^{-1}\alpha_2 u_2 - \cdots - \alpha_1^{-1}\alpha_r u_r.$$

これから $\langle v_{i_1}, u_2, \cdots, u_r\rangle \supseteqq \langle u_1, u_2, \cdots, u_r\rangle$. したがって $\{v_{i_1}, u_2, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\}$ である. さて $\{v_{i_1}, u_2, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\}$ より最初の主張を u_2 に適用して $\{v_{i_1}, v_{i_2}, u_3, \cdots, u_r\} \sim \{v_1, v_2, \cdots, v_s\}$. これを続けて, $\{v_{i_1}, v_{i_2}, \cdots, v_{i_r}\} \sim \{v_1, v_2, \cdots, v_s\}$ を得る. これと $v_1, v_2, \cdots, v_s$ の線型独立性から $r = s$ でなければならないことがわかる. ▮

V を有限生成として, $\{u_1, u_2, \cdots, u_m\}$ を V の生成系としよう. このとき $\{u_1, u_2, \cdots, u_m\}$ からベクトル $v_1, v_2, \cdots, v_n$ を適当に選んで

(β) $v_1, v_2, \cdots, v_n$ は k 上線型独立,

(γ) $V = \langle v_1, v_2, \cdots, v_n\rangle$

となるようにできる. 実際, つぎのようにして $u_1, u_2, \cdots, u_m$ から各 u_j を選びだすか否かを定めればよい: 最初に $u_1 \neq 0$ ならば u_1 を採用する. つぎに $u_1, u_2, \cdots, u_{l-1}$ まで選考が終っているとき $u_{i_1}, u_{i_2}, \cdots, u_{i_k}$ $(k \leqq l-1)$ が選びだされているものとして, $u_l \notin \langle u_{i_1}, u_{i_2}, \cdots, u_{i_k}\rangle$ ならば u_l を採用し, そうでなければ除く. かくして最終的に選びだされたベクトル $u_{i_1}, u_{i_2}, \cdots, u_{i_n}$ が (β), (γ) を満たすことは容易にわかる.

有限生成な線型空間 V に対し (β), (γ) を満たすベクトル $v_1, v_2, \cdots, v_n$ を V の

基底，n を V の**次元**といい，これを $\dim V$ あるいは $[V:k]$ で表わす．(α) により V の次元は V に対して一意的に定まる．

問 1.63　V を有限生成な線型空間とする．$u_1, u_2, \cdots, u_k$ が線型独立のとき，$u_1, u_2, \cdots, u_k$ を含む基底がとれる．U が V の部分空間ならば $\dim U \leqq \dim V$.

例 1.19　K を任意の斜体，L, M を K の部分斜体で $L \supseteqq M$ とする．このとき $[K:L][L:M]=[K:M]$ である．

[証明]　L を M 上の線型空間，K を L 上の線型空間と考えて，$\{u_1, u_2, \cdots, u_n\}$，$\{v_1, v_2, \cdots, v_m\}$ をそれぞれの基底とすると，$\{u_iv_j \mid 1 \leqq i \leqq n,\ 1 \leqq j \leqq m\}$ が K の M 上の基底であることが容易に確かめられる．▌

V, V' を斜体 k 上の線型空間とする．V から V' への写像 f が

$$\begin{aligned} f(u+v) &= f(u)+f(v), \\ f(\alpha u) &= \alpha f(u) \end{aligned} \qquad (\alpha \in k,\ u, v \in V)$$

なる条件を満たすとき，V から V' への**線型写像**という．とくに $V=V'$ のときこのような f を V の**線型変換**という．V の線型変換全体の集合を $\mathrm{End}(V)$ と書くと，$\mathrm{End}(V)$ はつぎの演算により環となる：$\mathrm{End}(V) \ni f, g$ に対して

$$(f+g)(u) = f(u)+g(u),$$

$$(*) \qquad (fg)(u) = g(f(u)) \qquad (\text{積の順序に注意}).$$

環 $\mathrm{End}(V)$ の乗法群を $GL(V)$ と書く．V が有限生成のとき，$\{u_1, u_2, \cdots, u_n\}$ をその基底とすると，$\mathrm{End}(V) \ni f$ に対して

$$f(u_i) = \sum_{j=1}^{n} a_{ij}u_j \qquad (1 \leqq i \leqq n)$$

によって，$A=(a_{ij}) \in M_n(k)$ を定めれば，$f \mapsto A$ なる対応により

$$(1.19) \qquad \mathrm{End}(V) \simeq M_n(k) \qquad (\text{環としての同型}),$$

$$(1.20) \qquad GL(V) \simeq GL_n(k) \qquad (\text{群としての同型})$$

となることが容易に確かめられる．

問 1.64　(1.19)，(1.20) を確かめよ．

注意　$\mathrm{End}(V) \ni f, g$ に対して

$$(**) \qquad fg(u) = f(g(u))$$

によって積を定義しても $\mathrm{End}(V)$ は環となる．しかしこのように積を定義すると，k が非可換ならば一般には同型 (1.19) は成立しない．すなわち $\mathrm{End}(V)$ には環としての構造が 2 通り定義し得るのであるが，(1.19) が成立するようにするには (*) のように定義し

なければならないのである．ただし k が可換体のときは，(**) によって積を定義しても (1.19) が成り立つ．このときは

$$f(u_j)=\sum_{i=1}^{n}a_{ij}u_i \qquad (1\leqq j\leqq n)$$

によって $(a_{ij})\in M_n(k)$ を定めればよい．

V の基底の集合と $GL(V)$ の間には1対1の対応がある．(ただし $\{u_1,u_2,\cdots,u_n\}$ を基底とするとき，$u_1,u_2,\cdots,u_n$ を並べる順序も考慮に入れる．したがって，たとえば $\{u_1,u_2,\cdots,u_n\}$ と $\{u_2,u_1,\cdots,u_n\}$ は異なる基底と考えるのである．) なぜなら，V の一つの基底 $\{e_1,e_2,\cdots,e_n\}$ を固定するとき，V の任意の基底 $\{u_1,u_2,\cdots,u_n\}$ に対して $f(e_i)=u_i$ なる $f\in GL(V)$ がただ一つ定まり，逆に $f\in GL(V)$ とすると $\{f(e_1),f(e_2),\cdots,f(e_n)\}$ は V の基底となるからである．

k が可換体のとき，$f\in\mathrm{End}(V)$ に対応する行列 A の行列式は V の基底のとり方によらない．したがって対応する行列の行列式を $f\in\mathrm{End}(V)$ の行列式という．

$$SL(V)=\{f\in\mathrm{End}(V)\mid\det f=1\}$$

とおけば，$SL(V)$ は $GL(V)$ の部分群であり

$$SL(V)\simeq SL_n(k)$$

が成り立つ．

k を任意の体とするとき，$M_n(k)$ の行列

$$R(i,j,c)=\begin{bmatrix}1 & & \vdots & & \vdots & & \\ & \ddots & \vdots & & \vdots & & \\ \cdots\cdots & & 1 & \cdots & c & \cdots\cdots & \\ & & \vdots & \ddots & \vdots & & \\ \cdots\cdots & & & \cdots & 1 & \cdots\cdots & \\ & & \vdots & & \vdots & \ddots & \\ & & \vdots & & \vdots & & 1\end{bmatrix}\begin{matrix}\\ \\ i\\ \\ j\\ \\ \\ \end{matrix} \qquad (c\in k)$$

(列 i, j)

は $SL_n(k)$ の生成系である．これは $k=\boldsymbol{C}$ のときとまったく同様にしてわかる．(§1.5問1.38参照.) この事実は第2章で $PSL(V)$ の単純性の証明において用いられるであろう．

さて最後にいままでのことの応用を与えよう．最初は"有限個の元からなる斜体の乗法群は Abel 群である"という Wedderburn の定理である．

定理 1.11 (Wedderburn)　有限個の元からなる斜体は可換体である.

証明　ここで述べるのは E. Witt による有名な証明である. それは群論的——斜体の乗法群の類等式を作る——前半と, 整数論的——その類等式が成立し得ないことを示す——後半に分れる.

K を有限個の元からなる斜体としよう. K が非可換体であると仮定して矛盾をだす.

$$Z=\{x\in K\,|\,xy=yx\ (\forall y\in K)\}$$

とおくと, Z は K の可換な部分体で乗法群 Z^* は K^* の中心である. K は非可換体と仮定しているから $K^*\neq Z^*$ である. $K^*-Z^*\ni\alpha$ をとり乗法群 K^* における α を含む共役類の元の数を調べる.

$$K_\alpha=\{x\in K\,|\,x\alpha=\alpha x\}$$

とおくと, K_α は Z を含む部分斜体である. $[K:Z]=n$, $[K_\alpha:Z]=d$ とおくと例 1.19 により $d|n$, $d\neq n$ である. また $|Z|=q$ とおくと, $|K_\alpha{}^*|=q^d-1$, $|K^*|=q^n-1$ であって $K_\alpha{}^*$ は K^* における α の中心化群にほかならないから, 定理 1.7 により α を含む共役類は $(q^n-1)/(q^d-1)$ 個の元を含む. したがって K^* の類等式はつぎの形となる:

$$(*)\qquad q^n-1=q-1+\sum_{\substack{d|n\\ d\neq n}}{}'\frac{q^n-1}{q^d-1}.$$

ただし, d は $d|n$, $d\neq n$ なるすべての d を走るわけではない. ここで $(*)$ が成り立ち得ない式であることを示せば証明は終る. このことを見るために円周等分多項式を利用する. $\zeta_n=\cos\dfrac{2\pi}{n}+\sqrt{-1}\sin\dfrac{2\pi}{n}$ として

$$F_n(X)=\prod_{(i,n)=1}(X-\zeta_n{}^i)$$

とおく. これを **n 次円周等分多項式**という. ところで

$(**)$　$F_n(X)$ は整数係数の多項式である

ことが知られている. (本選書"体と Galois 理論"参照.) さて明らかに

$$X^n-1=\prod_{i=1}^{n}(X-\zeta_n{}^i)=\prod_{l|n}F_l(X)$$

であるから, $F_n(X)$ は $(X^n-1)/(X^d-1)$ $(d|n,\ d\neq n)$ を割り, その商 $\prod_{\substack{l|n\\ l\nmid d}}F_l(X)$ は $(**)$ により整係数多項式である. したがって $F_n(q)$ は $(q^n-1)/(q^d-1)$ $(d|n,$

$d\neq n$) を割る．よって $(*)$ により $F_n(q)$ は $q-1$ を割らなければならない．とくに $|F_n(q)|\leqq q-1$ である．一方，容易にわかるように $|q-\zeta_n{}^i|>|q-1|$ $(i\neq n)$ だから，$|F_n(q)|>q-1$ が得られて矛盾となる．▌

例題 1.6　有限体の元の数は或る素数のベキである．

［証明］　有限体 K の標数を p とすると，p は素数である(例 1.18)．したがって K は $\boldsymbol{Z}_p$ (と同型な体) を含む．K を $\boldsymbol{Z}_p$ 上の線型空間と考えてその次元を n とすれば $|K|=p^n$ となる．▌

さて有限体に関してはつぎのことが知られている：

(1.21)　二つの有限体の元の数が等しければ，それらは同型である．

このことを示すには準備が必要なのでここでは省略する．詳しくは本選書“体と Galois 理論”参照．——

q 個の元からなる有限体を F_q とするとき，(1.21) によって F_q 上の一般線型群 $GL_n(F_q)$，特殊線型群 $SL_n(F_q)$ の構造は，n と q によって定まる．したがって $GL_n(F_q)$，$SL_n(F_q)$ をそれぞれ $GL(n,q)$，$SL(n,q)$ と書く．

例題 1.7　$GL(n,q)$，$SL(n,q)$ の位数はつぎのようになる：

$$|GL(n,q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1),$$
$$|SL(n,q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1).$$

［証明］　V を F_q 上の n 次元線型空間とする．$|GL(V)|$，$|SL(V)|$ を求めればよい．V の基底の集合と $GL(V)$ の間に 1 対 1 の対応があるから，V の基底が何通りできるかを数えれば $|GL(V)|$ が得られる．基底の最初のベクトル e_1 としては，$e_1\neq 0$ なる任意のベクトルが選べるから (問 1.63)，e_1 としては $|V-\{0\}|=q^n-1$ 通りの選び方がある．e_1 を選んだとき，e_2 として $V-\langle e_1\rangle$ の任意のベクトルが選べる．したがって e_2 の選び方は $|V-\langle e_1\rangle|=q^n-q$ 通りある．e_1,e_2 が選ばれているとき，e_3 は $V-\langle e_1,e_2\rangle$ の任意のベクトルが選べるから，e_3 の選び方は $|V-\langle e_1,e_2\rangle|=q^n-q^2$ 通りある．このことを続けて

$$|GL(V)| = (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$
$$= q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1)$$

を得る．$GL(V)$ から $F_q{}^*$ への写像

$$GL(V)\ni A\longmapsto \det A\in F_q{}^* \qquad (\det A \text{ は } A \text{ の行列式})$$

は $GL(V)$ から $F_q{}^*$ の上への準同型で，その核は $SL(V)$ である．準同型定理に

より

$$GL(V)/SL(V) \simeq F_q{}^*.$$

故に $|GL(V)|=|F_q{}^*|\cdot|SL(V)|=(q-1)|SL(V)|$. これから

$$|SL(V)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1)$$

を得る. ▌

$SL(n,q)$ に含まれるスカラー行列からなる $SL(n,q)$ の部分群を $Z(n,q)$ としよう:

$$Z(n,q) = \{\alpha E_n \mid \alpha \in F_q,\ \alpha^n=1\}.$$

$Z(n,q)$ は $SL(n,q)$ の中心である. $SL(n,q)$ の $Z(n,q)$ による剰余群を $PSL(n,q)$ によって表わす:

$$PSL(n,q) = SL(n,q)/Z(n,q).$$

$PSL(n,q)$ の位数は,

$$|PSL(n,q)| = \frac{1}{d}q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-1) \qquad (d \text{ は } n \text{ と } q-1 \text{ の最大公約数})$$

である. 定理1.9において n 次交代群 $\mathfrak{A}_n$ $(n\geqq 5)$ は有限単純群であることを証明したが, ここで定義した $PSL(n,q)$ も, $n=2,\ q=2$ または $n=2,\ q=3$ のときを除いて, 有限単純群である. われわれは, このことを§2.5において証明するであろう. また, つぎの場合に $\mathfrak{A}_n$ と $PSL(n,q)$ の位数が一致することが知られている:

$$|\mathfrak{A}_5| = |PSL(2,4)| = |PSL(2,5)| = 60,$$
$$|\mathfrak{A}_6| = |PSL(2,9)| = 360,$$
$$|\mathfrak{A}_8| = |PSL(4,2)| = |PSL(3,4)| = 20160.$$

これらは, $\mathfrak{A}_8$ と $PSL(3,4)$ の場合を除けば, 位数が一致するばかりでなく群が同型であることが知られている:

$$\mathfrak{A}_5 \simeq PSL(2,4) \simeq PSL(2,5),$$
$$\mathfrak{A}_6 \simeq PSL(2,9),$$
$$\mathfrak{A}_8 \simeq PSL(4,2).$$

これらの同型については, 第6章例6.4を参照. なお, $\mathfrak{A}_8$ と $PSL(3,4)$ は同型ではない. 読者自ら調べられたい.

第2章　群の集合への作用

群は置換群あるいは変換群の形で現われることが多い．歴史的にも群の概念はこのようにして現われてきた．本章では‘群の集合への作用’の概念を導き，置換群や変換群の基本事項とその応用を説明する．

§2.1　定義と例

G を群，Ω を集合とする．G が Ω に**作用する**とは，$G\times\Omega$ から Ω への写像

$$G\times\Omega \ni (g, x) \longmapsto g\circ x \in \Omega$$

が与えられていて

I　$G\ni g$ を固定するとき，Ω から Ω への写像

$$x \longmapsto g\circ x$$

は全単射である，

II　$1\circ x = x$　($\forall x\in\Omega$, 1 は G の単位元),

III　$(gg')\circ x = g\circ(g'\circ x)$

が成り立つことである．

問 2.1　IIはI, IIIからでることを示せ．また，II, IIIからIがでることを示せ．——

注意　上の定義の III は，写像 f, g の積の定義として

$$fg(x) = f(g(x))$$

を用いていることを意味している．しかし，§1.1例1.2の注意でも述べたように写像 f, g の積を

$$fg(x) = g(f(x))$$

とする方が便利なこともしばしば起る．このことに対応して，$\Omega\times G$ から Ω への写像

$$(x, g) \longmapsto x\circ g \qquad (x\in\Omega,\ g\in G)$$

が与えられていて

I′　$G\ni g$ を固定するとき，$x\mapsto x\circ g$ $(x\in\Omega)$ は Ω から Ω への全単射である，

II′　$x\circ 1 = x$　$(\forall x\in\Omega)$,

III′　$x\circ(gg') = (x\circ g)\circ g'$　$(x\in\Omega,\ g, g'\in G)$

が成り立つとき，G が Ω に作用するということがある．I-III と I′-III′ は，本質的内容はまったく同一で，写像の積の定義の違いからくる記法の違いがあるだけなのであるが，この両者を区別するために I-III が成り立つとき G は Ω に**左から作用する**といい，I′-III′ が成り立つとき G は Ω に**右から作用する**という．本講でもこれら両者をそのときの便宜に応じて使い分けるが，概念の構成はまったく同じなので断わらない限り I-III にしたがって話を進める．

問 2.2　G が Ω に右から作用しているとする．$G\ni g$, $\Omega\ni x$ に対して

$$g\circ x = x\circ g^{-1} \qquad (\text{右辺で左辺を定義する})$$

とおけば，G は Ω に左から作用する．——

群 G が集合 Ω に(左から)作用しているとしよう．

$$g\circ x = x \quad (\forall x\in\Omega) \Longrightarrow g=1$$

が成り立つとき，G は Ω に**忠実**に作用する，あるいは簡単に (G,Ω) は忠実であるという．

$$N=\{g\in G \mid g\circ x = x\ (\forall x\in\Omega)\}$$

とおくと，N は G の正規部分群である．この N を (G,Ω) の**核**という．$\bar{G}$ を G の N による剰余群とすると

$$\bar{g}\circ x = g\circ x \qquad (\bar{g}\ \text{は}\ g\ \text{を含む}\ N\ \text{の剰余類})$$

によって $\bar{G}$ は Ω に作用し，しかもこの作用が忠実であることは容易にわかる．

$\Omega\ni x, y$ に対して G の或る元 g が存在して

$$g\circ x = y$$

なる関係は，Ω 上の同値関係である．この同値関係による同値類を G の Ω への作用に関する**軌道**あるいは簡単に (G,Ω) の軌道という．Ω 自身が軌道であるとき，G は Ω に**可移**に作用する，あるいは (G,Ω) は可移であるという．すなわち，任意の $x, y\in\Omega$ に対して G の元 g が存在して $g\circ x=y$ となるとき，(G,Ω) は可移である．

$x\in\Omega$ に対して

$$H=\{g\in G \mid g\circ x = x\}$$

とおくと，H は G の部分群である．この H を x の**固定部分群**という．この H をしばしば G_x で表わす．

問 2.3　$G\ni g$, $\Omega\ni x$ のとき，$gG_xg^{-1}=G_{g\circ x}$ を示せ．とくに (G,Ω) が可移のとき，Ω の二つの点の固定部分群は互いに共役である．

例 2.1 $\Omega=\{1,2,\cdots,n\}$ の上の対称群は，自然に Ω に作用している．すなわち $\mathfrak{S}_n\ni\sigma$，$\Omega\ni i$ に対して

$$\sigma\circ i=\sigma(i)$$

である．この作用は忠実であり，また可移でもある．$\Omega\ni i$ の固定部分群は $n-1$ 個の文字 $\Omega-\{i\}$ の上の $n-1$ 次対称群である．一般に有限集合 Ω と Ω 上の対称群 $\mathfrak{S}(\Omega)$ の部分群 G が与えられたとき，G は Ω に自然に作用し，この作用は忠実である．このような G を Ω 上の**置換群**という．いいかえると有限群 G が有限集合 Ω の上に忠実に作用しているとき，G を Ω 上の置換群というのである．$|\Omega|$ を置換群 G の**次数**という．

例 2.2 H を G の部分群とする．H による左剰余類の集合 G/H に G をつぎのように作用させる：$G\ni g$，$G/H\ni xH$ に対して

$$g\circ(xH)=gxH$$

と定義すると，G は G/H に左から作用する．この作用は可移であり，xH の固定部分群は xHx^{-1} である．またこの作用の核は $\bigcap_{x\in G}xHx^{-1}$ である．この部分群は H に含まれる G の最大の正規部分群であるから，G の G/H への作用が忠実であるためには，H が G の単位群でない正規部分群を含まないことが必要十分である．K を G の任意の部分群とするとき，当然 K は G/H の上に作用している．このとき $(K,G/H)$ の xH を含む軌道の元は $kxH\,(k\in K)$ の形をしているから，$(K,G/H)$ の軌道は集合 KxH に含まれる H の左剰余類である．$X=\{x_\lambda H\mid\lambda\in\Lambda\}$ を $(K,G/H)$ の軌道の代表元の集合（各軌道から一つずつ元を選びだして作った集合）とすれば

$$(*)\quad G=\sum_\lambda Kx_\lambda H\quad \text{すなわち}\quad G=\bigcup_\lambda Kx_\lambda H,\quad Kx_\lambda H\cap Kx_{\lambda'}H=\phi\quad(\lambda\neq\lambda')$$

となる．一般に G の部分群 K,H が与えられたとき，$G\ni x,y$ に対して

$$kxh=y\qquad(\exists k\in K,\ \exists h\in H)$$

なる関係は，G の上の同値関係である．この同値関係による各同値類は KxH の形をしており，同値類の代表系を $\{x_\lambda\mid\lambda\in\Lambda\}$ とすれば $(*)$ が成り立つ．$(*)$ を G の K,H による**両側分解**という．すなわち G の K,H による両側分解が，$(K,G/H)$ の軌道への分解を与えるのである．なお，H の右剰余類の集合 $H\backslash G$ に G を右から作用させることができる：$G\ni g$，$H\backslash G\ni Hx$ に対して

$$Hx\circ g = Hxg.$$

この作用も可移であり，Hx の固定部分群は $x^{-1}Hx$ である．

例 2.3 V を体 k 上の $n+1$ 次元線型空間，$\boldsymbol{P}(V)$ を V の 1 次元部分空間全体の集合とする．$\boldsymbol{P}(V)$ を k 上の **$\boldsymbol{n}$ 次元射影空間**という．$GL(V)\ni T$, $\boldsymbol{P}(V)\ni x$ とすると，$T(x)$ も 1 次元部分空間だから，$GL(V)$ は $\boldsymbol{P}(V)$ に自然に作用する：

$$T\circ x = T(x).$$

$GL(V)$ の $\boldsymbol{P}(V)$ へのこの作用は可移である．実際，$\boldsymbol{P}(V)\ni x, y$，$x\neq y$ ならば $x=\langle v_1\rangle$，$y=\langle v_2\rangle$ と書くとき，v_1, v_2 は k 上線型独立であり，したがって $T(v_1)=v_2$ なる $T\in GL(V)$ が存在する．このとき $T\circ x=y$ である．この作用の核は V のスカラー変換 $v\mapsto \alpha v$ $(\alpha\in k^*)$ の全体 $Z(V)$ である．したがって $\boldsymbol{n}$ 次元射影線型群 $PGL(V)=GL(V)/Z(V)$ は，$\boldsymbol{P}(V)$ の上に忠実かつ可移に作用している．なお，$GL(V)$ は，線型空間 V の上に自然に作用しているが，この作用の軌道は，零ベクトルからなる 1 点集合 $\{0\}$ と $V-\{0\}$ である．

問 2.4 $SL(V)$ は $\boldsymbol{P}(V)$ の上に可移に作用することを示せ．

問 2.5 実直交群 $O(n)$ は，$n-1$ 次元球面 $S^{n-1}=\{(x_1, x_2, \cdots, x_n)\in \boldsymbol{R}^n \mid x_1{}^2+x_2{}^2+\cdots+x_n{}^2=1\}$ の上に

$$A\circ x = x^tA \qquad (x\in S^{n-1},\ A\in O(n),\ \text{右辺は行列の積})$$

によって可移に作用する．$SO(n)$ がすでに S^{n-1} の上に可移であることを示せ．

問 2.6 $\mathscr{H}=\{z\in \boldsymbol{C} \mid \mathrm{Im}(z)>0\}$ ($\mathrm{Im}(z)$ は複素数 z の虚数部分) とおく．$SL_2(\boldsymbol{R})\ni A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$，$\mathscr{H}\ni z$ に対して

$$A\circ z = \frac{az+b}{cz+d}$$

とおくと，$SL_2(\boldsymbol{R})$ は $\mathscr{H}$ の上に作用する．この作用は可移であることを示せ．また $\mathscr{H}\ni\sqrt{-1}$ の固定部分群を求めよ．

例 2.4 G を任意の群とする．$G\ni g, x$ に対して

$$g\circ x = gxg^{-1}$$

とおくと，G は G に左から作用する．この作用の軌道が共役類にほかならない．単位元のみからなる集合は一つの軌道であるから，G が単位群でない限りこの作用は可移ではない．$G\ni x$ の固定部分群は，x の中心化群 $C_G(x)=\{y\in G \mid xy=$

$yx\}$ である．またこの作用が忠実であるためには，G の中心 $Z(G)$ が単位群であることが必要十分である．

問 2.7 G が Ω に作用しているとする．$G \triangleright N$，X を N の一つの軌道とするとき，$g \circ X\ (g \in G)$ も N の軌道であることを示せ．——

つぎの簡単な定理は大切である．

定理 2.1 Ω_0 を (G, Ω) の一つの軌道とする．$\Omega_0 \ni a$，a の固定部分群を H とすると，Ω_0 と H の左剰余類の集合 G/H とはつぎの対応によって 1 対 1 に対応する：

$$\Omega_0 \ni x \circ a \longleftrightarrow xH \in G/H.$$

とくに (G, Ω) が可移のとき，Ω と G/H の間には 1 対 1 の対応がある．

証明 Ω_0 は軌道だから，$\Omega_0 \ni b$ に対して $x \circ a = b$ なる $G \ni x$ が存在する．このとき Ω_0 から G/H への写像 f を

$$f(b) = xH$$

によって定義する．この定義が $x \circ a = b$ なる x のとり方によらないことを見なければならないが，それは

$$\begin{aligned} x \circ a = y \circ a &\Leftrightarrow y^{-1} \circ (x \circ a) = y^{-1} \circ (y \circ a) = a \\ &\Leftrightarrow (y^{-1}x) \circ a = a \\ &\Leftrightarrow y^{-1}x \in H \\ &\Leftrightarrow xH = yH \end{aligned}$$

からわかる．またこれから f が単射であることもわかる．明らかに f は全射であるから定理が成り立つ．▌

系 有限群 G が有限集合 Ω に作用しているとき，各軌道に含まれる元の数は G の位数の約数である．——

定理 2.1 によれば，G が Ω に可移に作用しているとき，Ω と G/H (H は Ω の或る点の固定部分群) の間には 1 対 1 の対応があるのであるが，実際にはもっと強いことがいえる．一般に G_i が $\Omega_i\ (i=1, 2)$ に作用しているとき，G_1 から G_2 の上への同型 φ と Ω_1 から Ω_2 への全単射 ψ が存在して

$$\psi(g \circ x) = \varphi(g) \circ \psi(x) \qquad (\forall x \in \Omega_1,\ \forall g \in G_1)$$

が成り立つとき，(G_1, Ω_1) と (G_2, Ω_2) は**同型**であるという．さて (G, Ω) が可移で H を Ω の或る点の固定部分群とするとき，G を G/H に例 2.2 のように作用さ

せる．このとき，(G, Ω) と $(G, G/H)$ は同型である．

問 2.8　これを確かめよ．——

したがって群 G の可移な作用は，本質的には例2.2のようにして得られるものしかないのである．この意味で群がどのような集合に可移に作用するかは，まったく群自身の‘内部問題’であるということもできる．しかしながら，実際には例2.3のように或る群が幾何学的構造をもった集合に作用している場合には，その集合への群の作用の仕方とかその集合の幾何学的性質を通じて群の性質が導かれたり，逆に群の性質を通じて作用している集合の幾何学的性質が導かれたりすることが多い．本章でも今後そのようないくつかの例をみるであろう．

§2.2　有限群論への応用

有限群 G が有限集合に作用しているとき群の性質とかその作用の仕方から或る数量関係が生じ，それから有用な結果が得られることがある．そのような例を二，三あげよう．

定理 2.2　$|G|=p^a n$ ($a\geqq 1$，p は素数，n は p で割れてもよい) とする．このとき G の位数 p^a の部分群が存在する．もっとくわしく位数 p^a の部分群の数を $N(p^a)$ とすると，

$$N(p^a) \equiv 1 \pmod{p}$$

である．

証明　ここで述べる証明は，H. Wielandt によるものである．G の p^a 個の元からなる部分集合全体の集合を Ω とする：

$$\Omega = \{X \subseteq G \mid |X|=p^a\}.$$

$|\Omega|=\binom{p^a n}{p^a}$ である．$G \ni g$，$\Omega \ni X$ とすると，$gX=\{gx \mid x \in X\} \in \Omega$ であるから，G は Ω に自然に作用する．この作用の軌道を $\Omega_1, \Omega_2, \cdots, \Omega_t$ として，$\Omega_i \ni X_i$ とする．H_i を X_i の固定部分群

$$H_i = \{h \in G \mid hX_i = X_i\}$$

とすると，$H_i X_i = X_i$ であるから，X_i は H_i の右剰余類の和集合である．X_i に含まれる H_i の右剰余類の数を n_i とすると，

$$p^a = |X_i| = |H_i| n_i,$$

$$|H_i| = p^{u_i} \qquad (0 \leqq u_i \leqq a)$$

である．定理2.1により

$$|\Omega_i| = [G:H_i] = p^{a-u_i}n$$

であるから

$$(*) \qquad u_i < a \Leftrightarrow |\Omega_i| \equiv 0 \pmod{pn}$$

を得る．さらに

(**) $\quad u_i = a \Leftrightarrow |\Omega_i| = n$

$\Leftrightarrow$ Ω_i は位数 p^a の部分群をただ一つ含み，それを K_i とすると Ω_i は K_i の左剰余類全体の集合である．

実際，$u_i=a$ ならば，$|X_i|=|H_i|$ だから，X_i は H_i の或る右剰余類 H_ix_i $(x_i \in X_i)$ に等しい．$K_i=x_i^{-1}H_ix_i$ とおけば，K_i は位数 p^a の部分群で $K_i=x_i^{-1}X_i \in \Omega_i$ である．Ω_i は軌道だから K_i のすべての左剰余類を含み，$|\Omega_i|=n=[G:K_i]$ より，Ω_i は K_i の左剰余類全体の集合でなければならない．(**)は，とくに $u_i=a$ なる i の数が $N(p^a)$ に等しいことを示している．したがって(*)と合わせて，

$$(***) \qquad \binom{p^a n}{p^a} = |\Omega| = |\Omega_1|+|\Omega_2|+\cdots+|\Omega_t|$$

$$\equiv \sum_{u_i=a} n \pmod{pn}$$

$$\equiv N(p^a)n \pmod{pn}$$

を得る．一方，つぎの合同式

$$\binom{p^a n}{p^a} \equiv n \pmod{pn}$$

が成り立つ．ここではこの合同式を‘群論的’に証明するが，興味のある読者は直接的な証明を試みられたい．さて位数 $p^a n$ の巡回群は，定理1.5により位数 p^a の部分群をただ一つ持つ．したがって(***)を位数 $p^a n$ の巡回群の場合に適用して

$$\binom{p^a n}{p^a} \equiv n \pmod{pn}$$

を得る．この合同式と(***)から，$N(p^a) \equiv 1 \pmod{p}$ が成り立つことがわかる．∎

$|G|=p^a g'$, $(p, g')=1$ とすると，定理2.2により G の位数 p^a の部分群が少なくとも一つ存在する．このような部分群を G の **Sylow p 部分群**という．つぎの定理は，有限群のもっとも重要な性質である．

定理 2.3 (Sylow の定理)　G を有限群とする．

(i)　G の Sylow p 部分群が存在する．

(ii)　P を G の一つの Sylow p 部分群，Q を任意の p 部分群(位数 p べキの部分群)とすると，Q の或る共役は P に含まれる．とくに Sylow p 部分群はすべて共役である．

(iii)　Sylow p 部分群の数は，p を法として1に合同な $|G|$ の約数である．

証明　(i)は定理2.2で示されている．(iii)はつぎに示す(ii)および§1.2問1.18からわかる．(ii)を示そう．$\Omega=G/P$ とおく．Q を G/P に例2.2のように作用させる：$xP\mapsto axP\ (a\in Q)$．$(Q, G/P)$ の軌道を $\Omega_1, \Omega_2, \cdots, \Omega_t$ とすると

$$|\Omega| = |\Omega_1|+|\Omega_2|+\cdots+|\Omega_t|.$$

ところで，Q は p 部分群だから，定理2.1により $|\Omega_i|=p^{a_i}\ (a_i\geqq 0)$ である．一方，$|\Omega|=[G:P]$ は p と素だから，上の等式の両辺を比べて，或る i に対して $|\Omega_i|=1$ でなければならない．すなわち $\Omega_i=\{xP\}$．Ω_i は軌道だから

$$yxP = xP \qquad (\forall y\in Q)$$

である．これは

$$x^{-1}yx\in P \quad (\forall y\in Q) \quad \text{すなわち} \quad x^{-1}Qx\subseteq P$$

を示す．とくに Q も Sylow p 部分群ならば，位数を比べて $x^{-1}Qx=P$ である．▍

上の定理2.3の証明にはつぎのような簡単な原理が含まれている．覚えておくと便利である．なお，一般に位数が p のべキ(p は素数)の群を **p 群**という．

補題 2.1　p 群 G が有限集合 Ω に作用し，Ω の元の数は p と素とする．このとき G は Ω に固定点をもつ．すなわち G の任意の元 g に対して $g\circ a=a$ なる $a\in\Omega$ が存在する．

問 2.9　補題2.1を確かめよ．——

つぎの定理は p 群の基本性質の一つである．

定理 2.4　p 群 G の中心は単位群ではない：$Z(G)\neq 1$.

証明　G を G に例2.4のように作用させると，G は $\Omega=G-\{1\}$ の上に作用すると考えられる．Ω の元の数は p と素だから，補題2.1により G は固定点をも

つ．すなわち $gzg^{-1}=z$ $(\forall g\in G)$ なる $z\in\Omega=G-\{1\}$ が存在する．これは $Z(G)\neq 1$ を示す．▌

問 2.10 G を p 群，$G\triangleright N\neq 1$ ならば，$N\cap Z(G)\neq 1$.

例題 2.1 位数 p^2 の群は Abel 群である．

［証明］ G を位数 p^2 の群，$Z(G)=Z$ とおく．定理 2.4 により $Z\neq 1$. $G=Z$ ならば証明すべきことは何もない．よって $G\neq Z$ として矛盾を導こう．$G\neq Z$ とすると $[G:Z]=|Z|=p$. したがって $G-Z\ni a$ とすると，G の任意の元は a^iz $(0\leqq i\leqq p-1,\ z\in Z)$ と書ける．ところでこの形の二つの元は明らかに可換であるから，G は Abel 群すなわち $G=Z$ となり矛盾である．▌

例題 2.2 G を位数 pq の群（p,q は素数，$p>q$）とすると Sylow p 部分群は G の正規部分群である．$p\not\equiv 1 \pmod q$ ならば G は巡回群である．

［証明］ G の位数 pq の約数は

$$1,\quad p,\quad q,\quad pq$$

である．定理 2.3 (iii) により Sylow p 部分群の数は，これら四つの約数のうち p を法として 1 に合同なものであるが，$p>q$ に注意すればそれは 1 でなければならない．したがって Sylow p 部分群は正規部分群である．$p\not\equiv 1 \pmod q$ ならば，まったく同様の理由で Sylow q 部分群も正規部分群である．P, Q をそれぞれ G の Sylow p 部分群，Sylow q 部分群とし，$P=\langle a\rangle$，$Q=\langle b\rangle$ とする．$G\triangleright P$，$G\triangleright Q$ より

$$a^{-1}b^{-1}ab\in P\cap Q=1,$$
$$\therefore\quad ab=ba.$$

これから ab の位数が pq であることがわかる．▌

問 2.11 位数 45, 99 の群は Abel 群である．

問 2.12 §1.5 例 1.14 で構成された群 $Z(m,n,r,k)$ の m,n,r,k を適当にとり，位数 p^3 の非 Abel 群，位数 pq（p,q は素数，$p\equiv 1 \pmod q$）の非 Abel 群を作れ．

問 2.13 $SL(2,q)$ の Sylow 2 部分群は，q が偶数ならば Abel 群，q が奇数ならば 4 元数型の群であることを示せ．また $PSL(2,q)$ の Sylow 2 部分群は，q が偶数なら Abel 群，q が奇数ならば正 2 面体群である．

§2.3　原始的作用

一般論に戻る．群 G が集合 Ω に可移に作用しているとしよう．Ω の部分集合 X が，G の各元 g に対して

$$g\circ X = X \quad \text{または} \quad g\circ X\cap X = \phi$$

なる条件を満たすとき，X は (G, Ω) の**非原始ブロック**とよばれる．$\Omega=X$ あるいは X がただ1点からなる場合には，X は明らかに非原始ブロックであるが，これらは**自明な非原始ブロック**とよばれる．(G, Ω) が自明な非原始ブロックしかもたないとき，G の Ω への作用は**原始的**であるという．Ω の点の二つの順序づけられた任意の組 (a_1, a_2), (b_1, b_2) に対して

$$g\circ a_i = b_i \qquad (i=1,2)$$

を満たす $g\in G$ が存在するとき，G は Ω の上に**2重可移**に作用するという．n 次対称群 $\mathfrak{S}_n$ $(n\geqq 3)$，n 次交代群 $\mathfrak{A}_n$ $(n\geqq 4)$ は，$\Omega=\{1, 2, \cdots, n\}$ の上に2重可移に作用している．

補題 2.2　(G, Ω) が2重可移ならば，原始的である．

証明　X を (G, Ω) の自明でない非原始ブロックとする．$X\ni a, b$ $(a\neq b)$，$\Omega-X\ni c$ をとる．2重可移性により

$$g\circ a = a, \qquad g\circ b = c$$

なる $g\in G$ が存在する．このとき，$g\circ X\neq X$, $g\circ X\cap X\neq\phi$ であるが，これは X が非原始ブロックであることに反する．▌

例 2.5　V を体 k 上の有限次元線型空間 $(\dim V\geqq 2)$ とする．$GL(V)$ の $\boldsymbol{P}(V)$ への作用(例2.3)は2重可移，したがって補題2.2により原始的である．実際，$\boldsymbol{P}(V)\ni a_1, a_2, b_1, b_2$ $(a_1\neq a_2,\ b_1\neq b_2)$，$a_i=\langle v_i\rangle$，$b_i=\langle u_i\rangle$ $(i=1, 2,\ u_i, v_i\in V)$ とすると，v_1, v_2 と u_1, u_2 はそれぞれ線型独立な V のベクトルである．よって $T(v_i)=u_i$ $(i=1, 2)$ なる $T\in GL(V)$ が存在し，$T\circ a_i=b_i$ となる．なお，いま述べたことを注意深く見れば，V 上の特殊線型群 $SL(V)$ が $\boldsymbol{P}(V)$ の上に2重可移したがって原始的であることがわかる．また $PSL(V)=SL(V)/SL(V)\cap Z(V)$ ($Z(V)$ はスカラー変換全体の部分群)は $\boldsymbol{P}(V)$ の上に忠実かつ原始的である．$GL(V)$ あるいは $SL(V)$ を $V-\{0\}$ の上に自然に作用させると，$|k|>2$ ならばこの作用は非原始的である．なぜならば，1次元部分空間は明らかに自明でない非原始ブロックとなるからである．($|k|=2$ のときは $\boldsymbol{P}(V)=V-\{0\}$ に注意.)

例 2.6 実特殊直交群 $SO(n)$ の $n-1$ 次元球面 $S^{n-1}=\{(x_1, x_2, \cdots, x_n) \in \boldsymbol{R}^n \mid x_1^2+x_2^2+\cdots+x_n^2=1\}$ の上への作用

$$A\circ x = x^t A \qquad (x \in S^{n-1},\ A \in SO(n))$$

を考えよう．問 2.5 によりこの作用は可移である．しかしこの作用は原始的ではない．なぜなら，$X=\{x, -x\}$ $(x \in S^{n-1})$ が明らかに自明でない非原始ブロックとなるからである．しかし S^{n-1} の点 x と $-x$ を同一視したもの $\bar{x}$ の集合

$$\overline{S^{n-1}} = \{\bar{x}=\{x, -x\} \mid x \in S^{n-1}\}$$

の上に $A\circ\bar{x}=\overline{x^t A}$ によって $SO(n)$ を自然に作用させると，この作用は原始的である．ただし $n\geqq 3$ とする．これを見るには，X が $(SO(n), S^{n-1})$ の非原始ブロックで，$X=-X$, $X\neq\{x, -x\}$ のとき，$X=S^{n-1}$ をいえばよい．まず，つぎのことに注意する：

$$(\alpha) \quad \begin{array}{l} S^{n-1} \ni a_1, a_2, b_1, b_2, \\ (a_1, a_2) = (b_1, b_2) \end{array} \Longrightarrow \exists A \in SO(n), \quad A\circ a_i = b_i \quad (i=1, 2).$$

ここで (a_1, a_2), (b_1, b_2) は n 次元 Euclid 空間 $\boldsymbol{R}^n$ における内積を表わす．これは直観的には明らかであるが，正確に示すのは，いわゆる Schmidt の直交化の簡単な応用なので読者にまかせる．X を $(SO(n), S^{n-1})$ の上のような非原始ブロックとするとき，

(β) $X \ni a, b$ が存在して $(a, b)=0 \Longrightarrow X=S^{n-1}$

である．実際，$X\neq S^{n-1}$ として，$S^{n-1}-X \ni c$ をとると，$(a, x)=(c, x)=0$ なる $x \in S^{n-1}$ が存在する．このとき $a_1=b_1=a$, $a_2=b$, $b_2=x$ として (α) を適用すれば，$a \in A\circ X \cap X$, よって $A\circ X=X$, とくに $A\circ b=x \in X$ を得る．今度は，$a_1=a$, $a_2=b_1=x$, $b_2=c$ として (α) を適用すれば，$c \in X$ となり矛盾である．

以下，X が互いに直交するベクトルを含むことを示そう．$X\neq\{x, -x\}$ より X は $b\neq\pm a$ なる a, b を含む．必要ならば a, b の符号を変えて，a と b のなす角は $\pi/2$ 以下としてよい．a, b およびこれらと直交するベクトルによって生成される $\boldsymbol{R}^n$ の 3 次元部分空間 $\boldsymbol{R}^3$ と S^{n-1} の交わりである 2 次元球面 S^2 を考える．図 4 は $\boldsymbol{R}^3$ における a, b を含む平面 Π への S^2 の投影図である．A を通り b と直交する平面と S^2 の交わり l の上の点 u は，$(b, a)=(b, u)$ を満たすから，(α) により $u \in X$ となる．とくに $c=\overrightarrow{OC} \in X$ となる．a, b のなす角を θ とすると，$a, c \in X$ のなす角は 2θ だから，初めから a, b のなす角は $\pi/4$ 以上としてよい．この

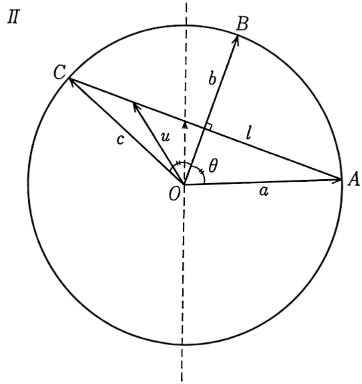


図4

とき原点を通り a と直交する平面と l の交わりの上の点を v とすると(a, b のなす角が $\pi/4$ 以上だから必ず交わることに注意)，$v \in X$, $(a, v)=0$ となる．したがって(β)により $X=S^{n-1}$ である．なお，$SO(n)$ の $\overline{S^{n-1}}$ の上への作用は，$SO(n)$ の $n-1$ 次元実射影空間の上への自然な作用(例2.3, 例2.5)を考えているに過ぎない．

補題2.3　(G, Ω) を可移とするとき，つぎの条件は同値である：

(i)　(G, Ω) は原始的である，

(ii)　1点の固定部分群は G の極大部分群である．ここで H が G の極大部分群とは，$G \supsetneq H_1 \supsetneq H$ なる部分群 H_1 が存在しないことである．

証明　(ii) $\Longrightarrow$ (i)：X を自明でない非原始ブロックとする．H を $X \ni a$ の固定部分群，$H_1=\{g \in G \mid g \circ X=X\}$ とおくと，H_1 は H を含む G の部分群である．$G \supsetneq H_1 \supsetneq H$ を示そう．(G, Ω) は可移で $\Omega \neq X$ であるから，$G \neq H_1$ である．一方，$X \ni b \neq a$ なる b および $g \circ a=b$ なる $g \in G$ が存在する．このとき，$gX \cap X \ni b$ より $g \circ X=X$. すなわち $g \in H_1$, また $a \neq b$ より $g \notin H$. したがって $H_1 \neq H$ である．

(i) $\Longrightarrow$ (ii)：H を $\Omega \ni a$ の固定部分群で，$G \supsetneq H_1 \supsetneq H$ なる部分群 H_1 が存在するとする．$X=\{h \circ a \mid h \in H_1\}$ とおくと，X は自明でない非原始ブロックである．実際，$H_1 \neq H$ より，$H_1-H \ni h$ とすれば，$h \circ a \neq a$. すなわち X は2点以上含む．また，$\Omega=X$ とすれば $g \in G-H_1$ に対して $g \circ a=h \circ a$ なる $h \in H_1$ が存在し，$h^{-1}g$

$\in H$. これは $g \in H_1$ を示すから矛盾である. ▌

補題 2.4　(G, Ω) は忠実かつ原始的とする. $G \triangleright N \neq 1$ とすると, N は Ω の上に可移である.

証明　N が Ω の上に可移でないとして, X を (N, Ω) の一つの軌道としよう. 以下, X が自明でない (G, Ω) の非原始ブロックであることを示す. (G, Ω) は忠実であるから, X は少なくとも 2 点を含む. また N は可移ではないと仮定しているから $\Omega \neq X$ である. 問 2.7 により, 任意の $g \in G$ に対して $g \circ X$ は N の軌道である. したがって $g \circ X = X$ または $g \circ X \cap X = \phi$ となる. ▌

§2.4　可解群と完全群

原始的作用の応用として, つぎの節で特殊射影線型群の単純性の証明を与える. しかしその証明に入る前に, これも群論における基本概念の一つである‘可解群’について説明しなければならない.

群 G はつぎの性質を持つ G の部分群の有限列 $G_0, G_1, \cdots, G_n$ が存在するとき**可解群**であるという:

(2.1)
$$G = G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1,$$
$$\left.\begin{array}{l} G_{i-1} \triangleright G_i, \\ G_{i-1}/G_i \text{ は Abel 群} \end{array}\right. \quad (i=1, 2, \cdots, n).$$

また

(2.2)
$$G \triangleright N, \quad G/N = \text{Abel 群} \implies G = N$$

なる条件を満たすとき, G を**完全群**という. 明らかに完全群は非可解群である.

補題 2.5　可解群の部分群, 剰余群は可解群である.

証明　G を可解群とすると, (2.1) を満たす部分群の有限列 $G_i\,(i=1, 2, \cdots, n)$ が存在する. H を G の部分群とすると $H_i = H \cap G_i$ は (2.1) を満たす H の部分群の列である. $H_{i-1} \triangleright H_i$ は明らかだから H_{i-1}/H_i が Abel 群であることを見ればよいが

$$H_{i-1}/H_i \simeq H \cap G_{i-1}/H \cap G_i \simeq H \cap G_{i-1}/(H \cap G_{i-1}) \cap G_i \simeq (H \cap G_{i-1})G_i/G_i$$

において最後の項は Abel 群 G_{i-1}/G_i の部分群だから, H_{i-1}/H_i も Abel 群である. なお上の式で最後の同型は第 2 同型定理 1.4 からでる. つぎに $G \triangleright N$ として $\bar{G} = G/N$ とおく. G から $\bar{G}$ への自然準同型による G_i の像を $\bar{G}_i$ とおくと,

この準同型は G_{i-1}/G_i から $\bar{G}_{i-1}/\bar{G}_i$ への準同型をひき起すから $\bar{G}_{i-1}/\bar{G}_i$ も Abel 群でなければならない．すなわち $\bar{G}$ の部分群の列 $\bar{G}_i$ は (2.1) を満たす．▍

補題 2.6　G が完全群であるためには

$$G = \langle x^{-1}y^{-1}xy \mid x, y \in G\rangle,$$

すなわち G が $x^{-1}y^{-1}xy$ の形の元全体で生成されることが必要十分である．とくにつぎの条件の一つが成り立てば，G は完全群である：

(i)　S を G の或る生成系とするとき，S の各元は $x^{-1}y^{-1}xy$ $(x, y \in G)$ と書ける，

(ii)　G の各共役類の代表元が $x^{-1}y^{-1}xy$ $(x, y \in G)$ の形に書ける．

証明　$G'=\langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$ とおく．G の任意の元 z に対して

$$(*)\qquad z^{-1}(x^{-1}y^{-1}xy)z = x'^{-1}y'^{-1}x'y' \qquad (x'=z^{-1}xz,\ \ y'=z^{-1}yz)$$

であるから $G' \triangleleft G$ である．$G \ni x, y$ に対して $x^{-1}y^{-1}xy \in G'$ より $xyG'=yxG'$．したがって G/G' は Abel 群である．したがって G が完全群ならば $G=G'$ でなければならない．逆に $G \triangleright N$, G/N が Abel 群とすると，G の任意の2元 x, y に対して

$$xNyN = yNxN \quad \text{すなわち} \quad xyN = yxN.$$

よって $x^{-1}y^{-1}xy \in N$. これから $G' \subseteqq N$. とくに $G=G'$ ならば $G=N$ となり，G は完全群となる．(i) が成り立てば，明らかに $G=G'$ であり G は完全群となる．(ii) が成り立てば，(＊) から G のすべての元が $x^{-1}y^{-1}xy$ の形に書けることになり，$G=G'$ となる．▍

一般に $G \ni x, y$ に対して $x^{-1}y^{-1}xy$ を x と y の**交換子**，$G'=\langle x^{-1}y^{-1}xy \mid x, y \in G\rangle$ を G の**交換子群**という．交換子や交換子群のいろいろな性質は，第5章でまとめて述べられる．

例 2.7　正2面体群，4元数型の群は可解群である．もっと一般に §1.5 例 1.14 で構成された群 $G=\boldsymbol{Z}(m, n, r, k)$ は可解群である．実際，例 1.14 の (1.17) の記号を用いて $N=\langle a\rangle$ とおくと，$G \triangleright N \triangleright 1$ で G/N と N は巡回群である．したがって $G=G_0$, $G_1=N$, $G_2=1$ とおけば，(2.1) を満たす．

例 2.8　n 次対称群は，$n \geqq 5$ のとき非可解群，$n \leqq 4$ ならば可解群である．$n \geqq 5$ ならば n 次交代群は完全群である．なぜなら，$n \geqq 5$ のとき n 次交代群 $\mathfrak{A}_n$ は定理 1.9 により非可換単純群であるから完全群とくに非可解群である．したがって

上の補題 2.5 により $n \geqq 5$ のとき $\mathfrak{S}_n$ は非可解群である．$n=1,2$ のとき $\mathfrak{S}_n$ はそれぞれ単位群，位数 2 の巡回群だから可解群である．$n=3$ のとき $\mathfrak{S}_3 \triangleright \mathfrak{A}_3 \triangleright 1$ なる列が (2.1) を満たす．$n=4$ とすると，

$$V = \{(1),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

は $\mathfrak{S}_4$ の正規部分群であることが容易に確かめられる．このとき，

$$\mathfrak{S}_4 \triangleright \mathfrak{A}_4 \triangleright V \triangleright 1$$

なる部分群の列は (2.1) を満たす．

4 次以下の対称群の可解性は，4 次以下の代数方程式が代数的に解ける（根が代数方程式の係数の加減乗除と根号を用いて表わせる）ことの群論的根拠を与える（本選書“体と Galois 理論”参照）．‘可解群’の名称の由来もここからでたものである．

例題 2.3　V を体 k 上の有限次元線型空間で，$\dim V \geqq 2$ とする．$SL(V)$ は完全群である．ただし $\dim V=2$ で k の元の数が 2 または 3 のときを除く：$(\dim V, |k|) \neq (2,2), (2,3)$．

［証明］　V に k 上の基底を定めて，$SL(V)$ を $SL_n(k)$ と同一視する．$SL_n(k)$ は

$$R(i,j,c) = \begin{bmatrix} 1 & & \vdots & & \vdots & & \\ & \ddots & \vdots & & \vdots & & \\ \cdots\cdots & & 1 & \cdots & c & \cdots\cdots & \\ & & \vdots & \ddots & \vdots & & \\ \cdots\cdots & & & \cdots & 1 & \cdots\cdots & \\ & & \vdots & & \vdots & \ddots & \\ & & \vdots & & \vdots & & 1 \end{bmatrix} \begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix} \qquad (c \in k)$$

（c は第 i 行第 j 列）

なる形の行列で生成される．行列の計算により

(α)　$n \geqq 3$ のとき

$$R(i,l,c)R(l,j,1)R(i,l,c)^{-1}R(l,j,1)^{-1} = R(i,j,c) \qquad (l \neq i,j),$$

(β)　$n=2$ でも

$$\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}^{-1}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & a(c^2-1) \\ 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} c^{-1} & 0 \\ 0 & c \end{bmatrix}\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}\begin{bmatrix} c^{-1} & 0 \\ 0 & c \end{bmatrix}^{-1}\begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 0 \\ a(c^2-1) & 1 \end{bmatrix} \qquad (c \in k^*,\ a \in k)$$

が成り立つ．$n \geqq 3$ のとき，(α) と補題2.6(i)により $SL_n(k)$ は完全群である．また $n=2$ でも，$|k|>3$ ならば $c^2-1 \neq 0$ なる $c \in k^*$ がとれるから，a, c を適当にとれば $a(c^2-1)$ は k の任意の元を表わす．(β) と補題2.6(i)により $n=2$ でも $|k|>3$ ならば $SL_n(k)$ は完全群である．▌

問 2.14　$SL(2,2)$，$SL(2,3)$ は可解群であることを示せ．

例題 2.4　$n \geqq 3$ のとき $SO(n)$ は完全群である．

［証明］　$SO(n)$ の共役類の代表元として

$$x = \begin{bmatrix} R(\theta_1) & & & & \\ & R(\theta_2) & & & \\ & & \ddots & & \\ & & & R(\theta_m) & \\ & & & & 1 \end{bmatrix}, \quad m = \begin{cases} \dfrac{n}{2} & (n\text{ が偶数のとき}), \\[2mm] \dfrac{n-1}{2} & (n\text{ が奇数のとき}), \end{cases}$$

$$R(\theta_i) = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix}$$

の形のものがとれる（n が偶数のとき右下隅の 1 はない）．

$$y = \begin{bmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & -1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix}$$

とおくと行列の計算により

$$y^{-1}x^{-1}yx = \begin{bmatrix} R(2\theta_1) & & & & & \\ & R(2\theta_2) & & & & \\ & & R(\theta_3) & & & \\ & & & \ddots & & \\ & & & & R(\theta_m) & \\ & & & & & 1 \end{bmatrix}$$

となる．これは，$SO(n)$ の各共役類の代表元が $y^{-1}x^{-1}yx$ の形となることを示すから，補題2.6(ii)を用いて $SO(n)$ が完全群であることがわかる．▌

問 2.15　$O(2)$ は可解群であることを示せ．

問 2.16　$SU(n)$ $(n \geqq 2)$ は完全群であることを示せ．

§2.5　$PSL(V)$ の単純性

本節では，§2.3, §2.4 の応用として $PSL(V)$ の単純性の証明をしよう．つぎの補題は，$PSL(V)$ ばかりではなく，いろいろな線型群の単純性の証明に用いられる．

補題 2.7　(G,Ω) を忠実かつ原始的とする．H を Ω の或る点の固定部分群として，つぎの条件を仮定する：

(i)　G は完全群，

(ii)　H は可解な正規部分群 K を含み，K の G における共役は G を生成する：$G=\langle xKx^{-1} \mid x\in G\rangle$.

このとき G は(非可換)単純群である．

証明　$G\triangleright N\neq 1$ のとき，$G=N$ を示せばよい．補題 2.4 により (N,Ω) は可移だから，$N\not\subseteq H$ である．また補題 2.3 により H は G の極大部分群だから，$G=NH$ でなければならない．(補題 1.1 により NH は G の部分群であることに注意.) したがって $H\triangleright K$ より $G=NH\triangleright NK$ を得る．一方，仮定により $G=\langle xKx^{-1} \mid x\in G\rangle$ だから，$G\triangleright NK$ より

$$G=\langle xKx^{-1} \mid x\in G\rangle \subseteq NK.$$

したがって

$$G=NK$$

となる．このとき

$$G/N=NK/N\simeq K/K\cap N \qquad (\text{第 2 同型定理}).$$

$G\neq N$ ならば左辺は完全群(完全群の剰余群は完全群である)，右辺は可解群(補題 2.5) とくに非完全群となり矛盾であるから，$G=N$ でなければならない．∎

定理 2.5　V を体 k 上の有限次元線型空間，$\dim V\geqq 2$ とする．$(\dim V,|k|)\neq(2,2),(2,3)$ のとき，$PSL(V)$ は非可換単純群である．

証明　ここで述べる証明は，K. Iwasawa によるものである．例 2.5 により $PSL(V)$ は射影空間 $\boldsymbol{P}(V)$ の上に忠実かつ原始的に作用する．また $(\dim V,|k|)\neq(2,2),(2,3)$ ならば例題 2.3 により $PSL(V)$ は完全群である．したがって $PSL(V)$ の 1 点の固定部分群について補題 2.7 の条件 (ii) が確かめられれば，定理の証明は完成する．V に k 上の基底を定めて $SL(V)$ と $SL_n(k)$ $(n=\dim V)$，V と k 上の n 項(行)ベクトルの空間 k^n を同一視する．V の 1 次元部分空間(すな

わち $\boldsymbol{P}(V)$ の元）として $\{(c,0,\cdots,0)\,|\,c\in k\}$ をとれば，この点の固定部分群 H は

$$\left[\begin{array}{c|ccc} a & * & \cdots & * \ \ * \\ \hline 0 & & & \\ \vdots & & A & \\ 0 & & & \end{array}\right]\in SL_n(k)$$

$$\qquad\qquad |\longleftarrow n-1 \longrightarrow|$$

なる形の行列からなる．

$$K=\left\{\left[\begin{array}{c|ccc} 1 & * & \cdots & * \ \ * \\ \hline 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{array}\right]\right\}$$

とおくと，$H\triangleright K$ かつ K は Abel 群とくに可解群で，$R(i,j,c)$ なる形の行列は K の元

$$\left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \ \ * \\ \hline 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{array}\right]$$

と $SL_n(k)$ で共役であることが容易に確かめられる（例1.11の記号で $Q(i,-1)\cdot P(i,j)$ の形の行列によって共役を作れ！）．これから補題2.7の条件(ii)が成り立つことがわかる．▌

補題2.7のもう一つの応用例をあげよう．

例題2.5　$SO(3)$ は単純群である．

［証明］　2次元球面 $S^2=\{(x,y,z)\,|\,x^2+y^2+z^2=1\}$ の直径の両端を同一視した点の集合 $\bar{S}$ の上に $SO(3)$ は原始的に作用する（例2.6）．この作用は忠実でもある．さらに例題2.4により $SO(3)$ は完全群である．$\bar{S}$ の点 $(0,0,\pm1)$ の固定部分群は

$$\begin{bmatrix} \pm R(\theta) & 0 \\ 0 & \pm1 \end{bmatrix}\qquad \left(R(\theta)=\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},\ \text{複号同順}\right)$$

でこれは可解群である．しかも $SO(3)$ の各共役類の代表元としてこの形のもの

がとれるから(例1.15)，補題2.7の条件(ii)が満たされる．以上により$SO(3)$の$\bar{S}$への作用は，補題2.7のすべての条件を満たし，したがって$SO(3)$は単純群である．▌

一般に$PSO(n)$ $(n \geqq 5)$，$PSU(n)$ $(n \geqq 2)$は単純群であることが知られている．($PSO(n)$，$PSU(n)$はそれぞれ$SO(n)$，$SU(n)$の中心による剰余群を表わす．$SO(2n+1)=PSO(2n+1)$!) しかし，これらを示すのに補題2.7を適用することはできない．たとえば$SO(n)$ $(n \geqq 4)$の場合，射影空間の上への作用(例2.6)は補題2.7の条件(ii)が成り立たないのである．しかし任意の体の上の斜交群や或る種の'直交群'，'ユニタリ群'に対して補題2.7が適用できて，それらの群(の交換子群の中心による剰余群)が単純群であることが示される．これらに興味のある方は，永尾汎著"群とデザイン"(岩波書店)を参照されたい．なお$PSO(4)$は単純群ではなく，

$$PSO(4) \simeq SO(3) \otimes SO(3)$$

であることが知られている．これは，

$$PSU(2) \simeq SO(3)$$

なる同型とともに，Hamiltonの4元数体を用いて示すことができるが，ここでは省略する．

§2.6　正則性と多重可移性

群Gが集合Ωに作用しているとする．Gの単位元でない任意の元がΩの上に固定点をもたないとき，(G,Ω)は**半正則**であるという．(G,Ω)が可移かつ半正則のとき**正則**という．

例2.9　Gを任意の群として，GをGにつぎのように作用させる：

$$g \circ x = gx \qquad (g, x \in G,\ \text{右辺は}\ G\ \text{における積}).$$

この作用は例2.2におけるGのG/Hへの作用において，Hを単位群とした場合にほかならない．この作用は正則であり，Gの**左正則表現**とよばれる．またGがΩに左から正則に作用しているとき，(G,Ω)はGの左正則表現と同型である．同様にGをGに右から

$$x \circ g = xg \qquad (x, g \in G)$$

によって作用させると，この作用も正則である．これはGの**右正則表現**とよば

れる.

問 2.17　(G, Ω) は忠実かつ可移とする. G が Abel 群ならば (G, Ω) は正則である.

問 2.18　(G, Ω) は忠実かつ原始的とする. N が G の可換な正規部分群ならば (N, Ω) は正則である.

問 2.19　(G, Ω) は忠実かつ可移, $N \lhd G$, (N, Ω) は正則とする. G_a を Ω の或る点 a の固定部分群とするとき, G_a を $N^\sharp = N - \{1\}$ の上に

$$g \circ x = gxg^{-1} \qquad (g \in G_a,\ x \in N^\sharp)$$

によって作用させると, $(G_a, \Omega - \{a\})$ と $(G_a, N^\sharp)$ は同型であることを示せ. ——

Ω の t 個の元の任意の順列 $(a_1, a_2, \cdots, a_t)$, $(b_1, b_2, \cdots, b_t)$ に対し, G の元 g が存在して

$$g \circ a_i = b_i \qquad (i=1, 2, \cdots, t)$$

なる条件が満たされるとき, (G, Ω) は **t 重可移**であるという. $t=1$ のときは (G, Ω) が可移であるということにほかならない. $t \geqq 2$ のとき (G, Ω) は**多重可移**であるという.

例 2.10　n 個の元からなる集合 Ω の上の対称群 $\mathfrak{S}(\Omega)$ は, Ω の上に n 重可移であり, Ω 上の交代群 $\mathfrak{A}(\Omega)$ $(n \geqq 4)$ は $n-2$ 重可移である. これらは**自明な多重可移群**とよばれる. V を或る体の上の有限次元線型空間 $(\dim V \geqq 2)$ とすると, $GL(V)$ の $\boldsymbol{P}(V)$ の上への作用は2重可移であった(例 2.5). $\dim V=2$ ならば, この作用は3重可移ですらあることが示される. このように2重可移群, 3重可移群は無限に存在するのであるが, 極めて著しい事実は4重以上の多重可移群は, 自明なものを除けば, いわゆる **Mathieu 群**とよばれる $M_{11}, M_{12}, M_{23}, M_{24}$ (添字は次数を表わす) のわずか四つしか知られていないことである. これら以外に4重以上の自明でない多重可移群が存在するかどうかは現在のところわかっていない. Mathieu 群は有限単純群の大切な実例であり, 興味深い性質も持っているのであるが定義などについてはここでは割愛せざるを得ない[1].

最後に原始性と多重可移性の関係についてふれてこの章を終りにしよう. 補題 2.2 によれば, (G, Ω) が多重可移ならば原始的である. この逆はもちろん成り立

---

1) 永尾汎: 群とデザイン, 岩波書店 (1974) 参照.

たないのであるが，これが成り立つための十分条件としてつぎの定理がある．

定理 2.6 (Jordan)　Ω を有限集合，(G,Ω) は原始的とする．Δ を Ω の部分集合で $1\leqq|\Delta|\leqq|\Omega|-2$ とし，

$$G_\Delta=\{g\in G\mid g\circ x=x\ (\forall x\in\Delta)\}$$

とおく．$(G_\Delta,\Omega-\Delta)$ が可移ならば，(G,Ω) は2重可移である．——

定理 2.6 の証明にはつぎの補題を用いる．

補題 2.8　Ω を有限集合，(G,Ω) は原始的とする．$\Omega\supsetneqq\Gamma$，$|\Gamma|\geqq2$ ならば，Γ の任意の2元 $a,b\ (a\neq b)$ に対して G の或る元 g が存在して $a\in g\circ\Gamma$，$b\notin g\circ\Gamma$ となる．

証明　$\Lambda=\bigcap_{a\in g\circ\Gamma}g\circ\Gamma$ とおき，Λ が非原始ブロックであることを示す．そのとき，(G,Ω) の原始性により，$\Lambda=\{a\}$ となるから補題の証明は終る．

$G\ni h$ に対して $a\in h\circ\Lambda$ とすると $h\circ\Lambda=\bigcap_{a\in g\circ\Gamma}hg\circ\Gamma$ より $h\circ\Lambda\supseteqq\Lambda$．$\Omega$ は有限集合だから元の数を比べて $h\circ\Lambda=\Lambda$．すなわち

$$(*)\qquad a\in h\circ\Lambda\quad(h\in G)\Longrightarrow h\circ\Lambda=\Lambda$$

である．つぎに $h\circ\Lambda\cap\Lambda\ni c$ とする．(G,Ω) の可移性により $k\circ a=c$ なる $k\in G$ が存在する．このとき，

$$a\in\Lambda\cap k^{-1}\circ\Lambda\cap k^{-1}h\circ\Lambda.$$

$(*)$ により $\Lambda=k^{-1}\circ\Lambda=k^{-1}h\circ\Lambda$，とくにあとの等式の両辺に k を掛けて $\Lambda=h\circ\Lambda$ を得る．これは Λ が非原始ブロックであることを示す．▌

定理 2.6 の証明　$|\Delta|$ に関する帰納法で証明する．$|\Delta|=1$ のとき，$\Delta=\{d\}$ とすれば仮定により d の固定部分群 G_d は $\Omega-\{d\}$ の上に可移である．これは (G,Ω) が2重可移であることを示す(つぎの問 2.20 参照)．以下 $|\Delta|\geqq2$ と仮定する．また $\Gamma=\Omega-\Delta$ とおく．以下 $2|\Delta|<|\Omega|$ と $2|\Delta|\geqq|\Omega|$ の二つの場合に分けて考える．

$2|\Delta|<|\Omega|$ の場合：補題 2.8 により $\Delta\ni a,b$，$G\ni g$ を適当にとり $a\in g\circ\Delta$，$b\notin g\circ\Delta$ とできる．$H=\langle G_\Delta,gG_\Delta g^{-1}\rangle$ とおくと，$G_\Delta,gG_\Delta g^{-1}$ がそれぞれ $\Gamma,g\circ\Gamma$ の上に可移であること(定理の仮定！)および $\Gamma\cap g\circ\Gamma\neq\phi$ ($2|\Delta|<|\Omega|$ より $2|\Gamma|>|\Omega|$ に注意)により，H は $\Gamma'=\Gamma\cup g\circ\Gamma$ の上に可移である．$\Omega-\Gamma'=\Delta\cap g\circ\Delta$ であるから H は $\Omega-\Gamma'$ の各点を固定する．したがって $\Delta'=\Omega-\Gamma'$ とおくと，Δ' は定理の仮定を満足し $b\notin g\circ\Delta$ により $|\Delta'|<|\Delta|$ である．よって数学的帰納法により (G,Ω) は2重可移である．

$2|\varDelta|\geqq|\varOmega|$ の場合：補題2.8により $\varGamma\ni a,b$, $G\ni g$ を適当にとれば, $a\in g\circ\varGamma$, $b\notin g\circ\varGamma$ とできる. $a\in\varGamma\cap g\circ\varGamma$ だから, $H=\langle G_\varDelta, gG_\varDelta g^{-1}\rangle$ は $\varGamma'=\varGamma\cup g\circ\varGamma$ の上に可移である. $2|\varGamma|<|\varOmega|$ だから $\varOmega\neq\varGamma'$. よって $\varDelta'=\varOmega-\varGamma'$ とおくと $\varDelta'\neq\phi$ で H は $\varDelta'=\varDelta\cap g\circ\varDelta$ の各点を固定する. したがって $\varDelta'$ は定理の仮定を満たし $b\notin\varDelta$ $b\in g\circ\varDelta$ より $|\varDelta'|<|\varDelta|$ であるから, 数学的帰納法により $(G,\varOmega)$ は2重可移である. ▌

例題 2.6 $\varOmega$ を有限集合, $(G,\varOmega)$ は忠実かつ原始的とする. G が少なくとも一つの互換を含めば $G=\mathfrak{S}(\varOmega)$ である.

[証明] $\varOmega=\{1,2,\cdots,n\}$, $G\ni(1\ 2)$ とする. $\varDelta=\{3,4,\cdots,n\}$ とおくと, $\varDelta$ は定理2.6の仮定を満たす. したがって $(G,\varOmega)$ は2重可移である. よって $\varOmega\ni i,j$ $(i\neq j)$ を任意にとると, $g\circ1=i$, $g\circ2=j$ なる $g\in G$ がとれる. このとき $g(1\ 2)g^{-1}=(i\ j)\in G$ となり, G は任意の互換を含む. $\mathfrak{S}(\varOmega)$ は互換全体で生成されるから $G=\mathfrak{S}(\varOmega)$ でなければならない. ▌

問 2.20 $(G,\varOmega)$ を可移とする. $\varOmega$ の或る点 d の固定部分群が $\varOmega-\{d\}$ の上に可移ならば, $(G,\varOmega)$ は2重可移であることを示せ.

問 2.21 $(G,\varOmega)$ は t 重可移とする. G が有限群ならば G の位数は $n(n-1)\cdots(n-t+1)$ $(n=|\varOmega|)$ で割れることを示せ.

第3章　単因子論と有限生成 Abel 群

本章では最初に(整数環上の)単因子論と有限生成 Abel 群の構造定理について述べる．これらの結果のほとんどすべては，主イデアル整域上の単因子論や有限生成加群に対して拡張され，それは応用上大切である．この拡張については，§3.4以降で説明する．

§3.1 単因子論

$M_{m,n}(\boldsymbol{Z})$ によって整数を成分とする m 行 n 列の行列全体の集合を表わす．$m=n$ のときは，$M_n(\boldsymbol{Z})$ と書く．環 $M_n(\boldsymbol{Z})$ の乗法群を $GL_n(\boldsymbol{Z})$ で表わす．$GL_n(\boldsymbol{Z})$ は整数を成分とする n 次行列で行列式が ± 1 のもの全体からなる群である．

$M_{m,n}(\boldsymbol{Z}) \ni A, B$ に対して，$GL_m(\boldsymbol{Z}) \ni X$，$GL_n(\boldsymbol{Z}) \ni Y$ が存在して

$$XAY = B \tag{3.1}$$

なる関係は，$M_{m,n}(\boldsymbol{Z})$ の上の同値関係である．本節ではこの同値関係による同値類の代表元の標準形を定める．

定理 3.1　同値関係(3.1)の各同値類はつぎの形の元をただ一つ含む：

$$\begin{bmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix} \qquad (e_1 | e_2 | \cdots | e_r,\ 0 < e_i \in \boldsymbol{Z}). \tag{3.2}$$

$M_{m,n}(\boldsymbol{Z}) \ni A$ を含む同値類が(3.2)の形の元を含むとき，$e_1, e_2, \cdots, e_r$ を A の**単因子**という．

標準形の存在証明

まず各同値類が(3.2)の形の元を含むことを示そう．証明の方法は，体の上の行列の基本変形の方法と同じである．つぎの形の3種類の正方行列を考える：

$$P(i,j)=\begin{bmatrix} 1 & & & \vdots & & & \vdots & & & \\ & \ddots & & \vdots & & & \vdots & & & \\ & & 1 & \vdots & & & \vdots & & & \\ \cdots & \cdots & \cdots & 0 & \cdots & \cdots & 1 & \cdots & \cdots & \cdots \\ & & & \vdots & 1 & & \vdots & & & \\ & & & \vdots & & \ddots & \vdots & & & \\ & & & \vdots & & & 1\ \vdots & & & \\ \cdots & \cdots & \cdots & 1 & \cdots & \cdots & 0 & \cdots & \cdots & \cdots \\ & & & \vdots & & & \vdots & 1 & & \\ & & & \vdots & & & \vdots & & \ddots & \\ & & & \vdots & & & \vdots & & & 1 \end{bmatrix}\begin{matrix} \\ \\ \\ i \\ \\ \\ \\ j \\ \\ \\ \\ \end{matrix},$$

$$Q_i=\begin{bmatrix} 1 & & & \vdots & & & \\ & \ddots & & \vdots & & & \\ & & 1 & \vdots & & & \\ \cdots & \cdots & \cdots & -1 & \cdots & \cdots & \cdots \\ & & & \vdots & 1 & & \\ & & & \vdots & & \ddots & \\ & & & \vdots & & & 1 \end{bmatrix}_i, \quad \begin{matrix} R(i,j,c)= \\ (c\in \boldsymbol{Z}) \end{matrix}\begin{bmatrix} 1 & & \vdots & & \vdots & & \\ & \ddots & \vdots & & \vdots & & \\ \cdots & \cdots & 1 & \cdots & c & \cdots & \cdots \\ & & \vdots & \ddots & \vdots & & \\ \cdots & \cdots & & \cdots & 1 & \cdots & \cdots \\ & & \vdots & & \vdots & \ddots & \\ & & \vdots & & \vdots & & 1 \end{bmatrix}\begin{matrix} \\ \\ i \\ \\ j \\ \\ \\ \end{matrix}.$$

これらは行列の次数が m ならば $GL_m(\boldsymbol{Z})$ の元である．$A\in M_{m,n}(\boldsymbol{Z})$ にこれらの行列を左から掛けることは，A に対してつぎの操作を行なうことを意味する：

(i)　第 i 行と第 j 行を入れかえる,

(ii)　第 i 行を -1 倍する,

(iii)　第 i 行に第 j 行の c 倍を加える.

また A に上の形の n 次行列を右から掛けることは,

(i)′　第 i 列と第 j 列を入れかえる,

(ii)′　第 i 列を -1 倍する,

(iii)′　第 j 列に第 i 列の c 倍を加える

なる操作を行なうことに相当する．以下 (i)-(iii)，(i)′-(iii)′ なる六つの操作を $A\in M_{m,n}(\boldsymbol{Z})$ にほどこして，A が (3.2) の形に変形されることを示そう．正確のために，$M_{m,n}(\boldsymbol{Z})$ の上の同値関係 (3.1) を少し変えて $M_{m,n}(\boldsymbol{Z})$ の二つの行列が

“(i)-(iii)，(i)′-(iii)′ なる六つの操作を何回かほどこして互いに移れる”

という同値関係を考える．（実は，この同値関係が最初に定義した同値関係(3.1)と同じものであることは後にわかる(例題3.1参照).）さてΩをこの同値関係による一つの同値類としよう．Ωは0でない行列を含むとしてよい．そこでΩに含まれる行列の成分として現われる0でない整数全体の集合を考え，その中で絶対値最小の整数をe_1とする．必要ならば(ii)あるいは(ii)$'$の操作をほどこして$e_1>0$としてよい．e_1を成分にもつΩの行列をAとしよう．e_1がAの(i,j)成分であれば，Aの第1行と第i行を入れかえ，さらに第1列と第j列を入れかえれば，e_1が(1,1)成分にある行列A'が得られる．$A'\in\Omega$である．

$$A'=\begin{bmatrix} e_1 & a_{12} & \cdots & a_{1n} \\ a_{21} & & & \vdots \\ \vdots & & & \\ a_{m1} & & \cdots & a_{mn} \end{bmatrix}$$

としよう．$a_{1j}\ (j>1)$をe_1で割って$a_{1j}=qe_1+s\ (0\leqq s<e_1)$とする．$A$の第$j$列から第1列の$q$倍を引くと$(1,j)$成分が$s$の行列$A''$が得られ，$A''\in\Omega$である．$s>0$ならば，$e_1>s$より$e_1$のとり方(最小性)に反するから$A''$の$(1,j)$成分は0でなければならない．各$j\ (j>1)$に対して同じことを行なえば，結局第1行の成分が$e_1$を除いてすべて0である$\Omega$の行列$A'''$が得られる．つぎに$A'''$に同じことを行に対して行なうことによって$\Omega$はつぎの形の行列を含むことがわかる：

$$\Omega\ni A_1=\left[\begin{array}{c|ccc} e_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A_1' & \\ 0 & & & \end{array}\right],\qquad A_1'\in M_{m-1,n-1}(\boldsymbol{Z}).$$

A_1'はAよりも次数の小さい行列であるから，A_1'に(i)-(iii)，(i)$'$-(iii)$'$をほどこして

$$A_1''=\begin{bmatrix} e_2 & & & & & & \\ & e_3 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}\qquad (e_2\,|\,e_3\,|\cdots|\,e_r,\ \ 0<e_i\in\boldsymbol{Z})$$

となる (数学的帰納法). A_1' をこの形にする操作を A_1 の第2列-第 n 列, 第2行-第 m 行にほどこせば,

$$A_2 = \begin{bmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

なる形の Ω の行列が得られる. $e_1|e_2$ を示せば標準形の存在証明は終る. e_2 を e_1 で割って $e_2=qe_1+s$ $(0\leqq s<e_1)$ とすると A_2 の第2行に第1行を加え, さらに第1列の q 倍を第2列から引くと,

$$\begin{bmatrix} e_1 & * & & & & & & \\ * & s & & & & & & \\ & & e_3 & & & & & \\ & & & \ddots & & & & \\ & & & & e_r & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 0 \end{bmatrix}$$

なる形の Ω の行列が得られるが, e_1 の最小性により $s=0$ でなければならない. すなわち $e_1|e_2$ である.

標準形の一意性

$M_{m,n}(\boldsymbol{Z}) \ni A$, $l=\max(m,n)$ とする. $l\geqq k\geqq 1$ に対して A のすべての k 次小行列式の最大公約数を $d_k(A)$ とする. ただし, k 次小行列式がすべて0のときは $d_k(A)=0$ とおく. $d_k(A)$ を A の **k 次小行列式因子**という. A の階数を r とすると,

(3.3)　　$d_1(A)\,|\,d_2(A)\,|\cdots|\,d_r(A), \qquad d_k(A)=0 \qquad (l\geqq k>r)$

である.

問 3.1　(3.3) を確かめよ. ——

標準形の一意性の証明にはつぎの補題を用いる.

補題 3.1　$M_{m,n}(\boldsymbol{Z}) \ni A, B$ が同値関係 (3.1) の同じ同値類に属するならば,

$$d_i(A) = d_i(B) \qquad (1 \leqq i \leqq l)$$

である.

証明 $M_{m,n}(\boldsymbol{Z}) \ni A$, $GL_m(\boldsymbol{Z}) \ni X$ のとき, $d_k(A) \mid d_k(XA)$ を示す. XA の k 次小行列は, X の或る k 個の行を選んで作った k 行 m 列の行列 X' と, A の或る k 個の列を選んで作った m 行 k 列の行列 A' の積 $X'A'$ の形をしている. $\det X'A'$ に補題 1.6 を適用すれば, $d_k(A) \mid \det X'A'$ を得る. これは, $d_k(A) \mid d_k(XA)$ を示す. 同様に $M_{m,n}(\boldsymbol{Z}) \ni A$, $GL_n(\boldsymbol{Z}) \ni Y$ のとき $d_k(A) \mid d_k(AY)$ である. 合わせて $d_k(A) \mid d_k(XAY)$. したがって, $A = X^{-1}(XAY)Y^{-1}$ より $d_k(XAY) \mid d_k(A)$. よって $d_k(A) = d_k(XAY)$ を得る. ▌

$M_{m,n}(\boldsymbol{Z}) \ni A$ を含む同値類の代表元の標準形を

$$A' = \begin{bmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix} \qquad (e_1 \mid e_2 \mid \cdots \mid e_r,\ 0 < e_i \in \boldsymbol{Z})$$

としよう. このとき明らかに

$$d_i(A') = e_1 e_2 \cdots e_i \qquad (1 \leqq i \leqq r).$$

補題 3.1 により $d_i(A) = d_i(A')$ であるから, $d_i(A) = e_1 e_2 \cdots e_i$ $(1 \leqq i \leqq r)$. これは A の単因子 $e_1, e_2, \cdots, e_r$ が A によって一意的に定まることを示している. これで標準形の一意性が証明された. ——

標準形の存在証明から, $GL_n(\boldsymbol{Z})$ の生成系についてつぎのことがわかる.

例題 3.1 $P(i,j)$, Q_i, $R(i,j,c)$ なる形の行列全体の集合は, $GL_n(\boldsymbol{Z})$ の生成系である.

[証明] $P(i,j)$, Q_i, $R(i,j,c)$ の形の行列全体の集合を S とする. $GL_n(\boldsymbol{Z}) \ni A$ ならば, A の単因子は $\underbrace{1, 1, \cdots, 1}_{n}$ でなければいけないから, A は (i)-(iii), (i)$'$-(iii)$'$ なる操作をほどこして単位行列となる. すなわち

$$X_1 X_2 \cdots X_s A Y_1 Y_2 \cdots Y_t = E_n \qquad (X_i,\ Y_i \in S)$$

となる. したがって

$$A = X_s^{-1} X_{s-1}^{-1} \cdots X_1^{-1} Y_t^{-1} Y_{t-1}^{-1} \cdots Y_1^{-1}.$$

これは S が $GL_n(\boldsymbol{Z})$ の生成系であることを示す. ▌

問 3.2　$GL_n(\boldsymbol{Z})$, $SL_n(\boldsymbol{Z})$ は有限生成である. もっとくわしく, $GL_n(\boldsymbol{Z})$ は $R(i,j,1)$, Q_n で生成され, $SL_n(\boldsymbol{Z})$ は $R(i,j,1)$ で生成されることを示せ.

[ヒント]　$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1}.$

§3.2　自由加群

本章では Abel 群の演算を加法で書き, Abel 群を加群とよぶ. 加群 G がつぎの条件を満たすとき, 階数 n の**自由加群**という:

(3.4)　G の n 個の元 $u_1, u_2, \cdots, u_n$ が存在して, G の各元は

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n \qquad (a_i \in \boldsymbol{Z})$$

の形に一意的に書ける.

このような $u_1, u_2, \cdots, u_n$ を自由加群 G の**基底**という. $\boldsymbol{Z}^n$ は階数 n の自由加群である. 実際 $\boldsymbol{Z}^n \ni e_i = (0, \cdots, 0, \overset{i}{\breve{1}}, 0, \cdots, 0)$ は (3.4) を満たす. G を階数 n の自由加群, $u_1, u_2, \cdots, u_n$ をその基底とするとき, G から $\boldsymbol{Z}^n$ への写像

$$G \ni a_1u_1 + a_2u_2 + \cdots + a_nu_n \longmapsto (a_1, a_2, \cdots, a_n) \in \boldsymbol{Z}^n$$

は, G から $\boldsymbol{Z}^n$ の上への同型である. すなわち階数 n の自由加群とは, $\boldsymbol{Z}^n$ に同型な群にほかならない.

ここで自由加群の階数が一意的に定まることを注意しておこう. すなわち $u_1, u_2, \cdots, u_n$ と $v_1, v_2, \cdots, v_m$ がともに (3.4) を満たすとき $m=n$ を確かめるのである.

$$u_i = \sum_{j=1}^{m} a_{ij}v_j \qquad (1 \leqq i \leqq n),$$

$$v_i = \sum_{j=1}^{n} b_{ij}u_j \qquad (1 \leqq i \leqq m)$$

によって $A = (a_{ij}) \in M_{n,m}(\boldsymbol{Z})$, $B = (b_{ij}) \in M_{m,n}(\boldsymbol{Z})$ を定め, 上の第2式を第1式に代入すると, (3.4) を用いて $AB = E_n$ を得る. このとき補題 1.6 を用いて $n \leqq m$ を得る. 同様に第1式を第2式に代入すれば $BA = E_m$, よって $m \leqq n$ を得るから $m=n$ でなければならない.

補題 3.2　G を階数 n の自由加群, $u_1, u_2, \cdots, u_n$ をその基底, $v_1, v_2, \cdots, v_n$ を G の任意の n 個の元とする. また,

$$v_i = \sum_{j=1}^{n} a_{ij} u_j \qquad (1 \leqq i \leqq n)$$

によって $A=(a_{ij}) \in M_n(\boldsymbol{Z})$ を定める．このとき，$v_1, v_2, \cdots, v_n$ が G の基底であるためには $A \in GL_n(\boldsymbol{Z})$ であることが必要十分である．

問 3.3　補題 3.2 を証明せよ．——

つぎの補題は自由加群の取り扱いにおいて基本的である．

補題 3.3　F_n を階数 n の自由加群，$u_1, u_2, \cdots, u_n$ をその基底とする．

(i) G を n 個の元で生成される任意の加群とすると，F_n から G の上への準同型が存在する．もっとくわしく，$G=\langle v_1, v_2, \cdots, v_n \rangle$ ならば，F_n から G の上への準同型 φ で $\varphi(u_i)=v_i$ $(1 \leqq i \leqq n)$ なるものが存在する．

(ii) G は任意の加群とし，φ を G から F_n の上への準同型とする．$\mathrm{Ker}\,\varphi=N$ とおくと，G の部分群 H が存在して

$$G = N+H, \qquad N \cap H = \{0\}, \qquad H \simeq F_n$$

となる．

証明　(i) F_n から G への写像

$$F \ni a_1u_1+a_2u_2+\cdots+a_nu_n \longmapsto a_1v_1+a_2v_2+\cdots+a_nv_n \in G$$

が求める準同型である．(ii) $\varphi(v_i)=u_i$ $(1 \leqq i \leqq n)$ なる $v_i \in G$ をとり，$H=\langle v_1, v_2, \cdots, v_n \rangle$ とおく．このとき，

$$(*) \qquad \varphi(a_1v_1+a_2v_2+\cdots+a_nv_n) = 0 \Longrightarrow a_1\varphi(v_1)+\cdots+a_n\varphi(v_n) = 0$$
$$\Longrightarrow a_1u_1+a_2u_2+\cdots+a_nu_n = 0$$
$$\Longrightarrow a_1 = a_2 = \cdots = a_n = 0$$

である．とくに

$$a_1v_1+a_2v_2+\cdots+a_nv_n = 0 \Longrightarrow a_1 = a_2 = \cdots = a_n = 0$$

が成り立つ．これは H が階数 n の自由加群であることを示す：$H \simeq F_n$．$G \ni x$, $\varphi(x)=a_1u_1+a_2u_2+\cdots+a_nu_n$ とすると $x-(a_1v_1+a_2v_2+\cdots+a_nv_n) \in N=\mathrm{Ker}\,\varphi$．したがって $G=N+H$ となる．$H \cap N=\{0\}$ は $(*)$ からでる．▌

定理 3.2　階数 n の自由加群の部分群は階数が高々 n の自由加群である．

証明　無限巡回群の 0 でない部分群は無限巡回群であるから，階数 1 のときは定理が正しいことに注意する．F_n を階数 n の自由加群，$u_1, u_2, \cdots, u_n$ をその基底，H を F_n の部分群とする．

$$F_i = \langle u_1, u_2, \cdots, u_i \rangle \qquad (1 \leqq i \leqq n),$$
$$H_i = H \cap F_i$$

とおく．以下 H_i は0または階数が高々 i の自由加群であることを示そう．とくに $H=H_n$ であるから，これは定理が成り立つことを示す．$H_1 \neq 0$ ならば，H_1 は階数1の自由加群 F_1 の部分群だから，最初の注意により H_1 は階数1の自由加群である．$i>1$ とする．H_i の元は，

$$x = y + au_i \qquad (y \in F_{i-1},\ a \in \boldsymbol{Z})$$

の形に一意的に書け，H_i から $\boldsymbol{Z}$ への写像 φ

$$\varphi:\ x \longmapsto a$$

は H_i から $\boldsymbol{Z}$ への準同型である．$\varphi(H_i)=0$ ならば，$H_i=H_{i-1}$ となり数学的帰納法の仮定により H_{i-1} は階数高々 $i-1$ の自由加群だから H_i もそうである．$\varphi(H_i) \neq 0$ とすると，$\varphi(H_i)$ は $\boldsymbol{Z}$ の0でない部分群だから階数1の自由加群である．補題3.3(ii)を適用して($H_{i-1}=\mathrm{Ker}\,\varphi$ に注意)

$$H_i = H_{i-1} + U_i, \qquad H_{i-1} \cap U_i = \{0\}, \qquad U_i \simeq \varphi(H_i) \simeq \boldsymbol{Z}$$

である．これから $U_i=\langle u_i' \rangle$ とすると，H_{i-1} の基底と u_i' が H_i の基底となることがすぐにわかるから，H_i は階数が高々 i の自由加群となる．∎

定理 3.3 F_n を階数 n の自由加群，H を F_n の階数 r の部分群($r \leqq n$)とする．F_n の基底 $u_1, u_2, \cdots, u_n$ を適当にとると，

$$e_1u_1,\ e_2u_2,\ \cdots,\ e_ru_r \qquad (e_1 \mid e_2 \mid \cdots \mid e_r,\ 0<e_i \in \boldsymbol{Z})$$

が H の基底となるようにできる．

証明 $u_1, u_2, \cdots, u_n$ を F_n の基底，$v_1, v_2, \cdots, v_r$ を H の基底としよう．

$$v_i = \sum_{j=1}^{n} a_{ij}u_j \qquad (1 \leqq i \leqq r,\ a_{ij} \in \boldsymbol{Z}),$$
$$A = (a_{ij}) \in M_{r,n}(\boldsymbol{Z})$$

とおくと，$v_1, v_2, \cdots, v_r$ の独立性により行列 A の階数は r である．定理3.1により $GL_r(\boldsymbol{Z}) \ni X,\ GL_n(\boldsymbol{Z}) \ni Y$ が存在して

$$XAY = \left[\begin{array}{cccc|c} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & 0 \\ & & & e_r & \end{array}\right] \in M_{r,n}(\boldsymbol{Z}) \qquad (e_1 \mid e_2 \mid \cdots \mid e_r,\ 0<e_i \in \boldsymbol{Z})$$

となる．

$$u_i' = \sum_{j=1}^{n} y_{ij} u_j, \qquad Y^{-1} = (y_{ij}) \in GL_n(\boldsymbol{Z}),$$

$$v_i' = \sum_{j=1}^{r} x_{ij} v_j, \qquad X = (x_{ij}) \in GL_r(\boldsymbol{Z})$$

とおくと，補題 3.2 により $(v_1', v_2', \cdots, v_r')$，$(u_1', u_2', \cdots, u_n')$ はそれぞれ H, F_n の基底であり，

$$v_j' = e_j u_j' \qquad (1 \leqq j \leqq r)$$

となる．▌

問 3.4 $\boldsymbol{Z} \ni a_1, a_2, \cdots, a_n$ $(n \geqq 2)$ とする．つぎの条件は同値であることを示せ：

(i) $(a_1, a_2, \cdots, a_n) = 1$ $(a_1, a_2, \cdots, a_n$ は互いに素$)$，

(ii) 数ベクトル $(a_1, a_2, \cdots, a_n)$ を含む $\boldsymbol{Z}^n$ の基底が存在する，

(iii) $a_1, a_2, \cdots, a_n$ を第 1 行 (あるいは第 1 列) とする $SL_n(\boldsymbol{Z})$ の元が存在する．

§3.3 有限生成 Abel 群

本節では，有限生成 Abel 群の構造を調べる．つぎの定理は，しばしば **'Abel 群の基本定理'** とよばれる．

定理 3.4 有限生成加群はいくつかの巡回群の直和と同型である．もっとくわしく，任意の有限生成加群 G に対して，

$$e_1 | e_2 | \cdots | e_r \qquad (1 < e_i \in \boldsymbol{Z})$$

なる整数 $e_1, e_2, \cdots, e_r$ と整数 $s \geqq 0$ が存在して，G は位数 e_i の巡回群 $\boldsymbol{Z}_{e_i}$ $(1 \leqq i \leqq r)$ と階数 s の自由加群 $\boldsymbol{Z}^s$ の直和に同型である：

$$G \simeq \boldsymbol{Z}_{e_1} \oplus \boldsymbol{Z}_{e_2} \oplus \cdots \oplus \boldsymbol{Z}_{e_r} \oplus \boldsymbol{Z}^s.$$

証明 有限生成加群 G が n 個の元で生成されているとする．F を階数 n の自由加群とすれば，補題 3.3 により F から G の上への準同型 φ が存在する．φ の核を H とすれば準同型定理により

$$F/H \simeq G.$$

さて H は自由加群 F の部分群であるから，定理 3.3 により F の基底 $u_1, u_2, \cdots, u_n$ を適当にとると

$$e_1' u_1, \ e_2' u_2, \ \cdots, \ e_t' u_t$$

が H の基底で $e_1' | e_2' | \cdots | e_t'$ となる．$F_i = \langle u_i \rangle$ $(1 \leqq i \leqq n)$，$H_i = \langle e_i' u_i \rangle$ $(1 \leqq i \leqq$

t), $H_j=0$ $(t<j\leqq n)$ とおけば,

$$F \simeq F_1\oplus\cdots\oplus F_n,$$
$$H \simeq H_1\oplus\cdots\oplus H_n$$

だから,

$$F/H \simeq F_1/H_1\oplus\cdots\oplus F_n/H_n.$$

ところで,

$$F_i/H_i \simeq \boldsymbol{Z}_{e_i'} \qquad (1\leqq i\leqq t),$$
$$F_j/H_j \simeq \boldsymbol{Z} \qquad (t<j\leqq n).$$

したがって $e_1'=e_2'=\cdots=e_p'=1$, $1<e_{p+1}'\leqq\cdots\leqq e_t'$ とするとき,

$$r=t-p, \quad s=n-t, \quad e_i=e_{p+i}' \quad (1\leqq i\leqq r)$$

とおけば,

$$F/H \simeq \boldsymbol{Z}_{e_1}\oplus\boldsymbol{Z}_{e_2}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}\oplus\underbrace{\boldsymbol{Z}\oplus\cdots\oplus\boldsymbol{Z}}_{s},$$

$$e_1\,|\,e_2\,|\cdots|\,e_r, \qquad e_i>1$$

となる. ▌

一般に Abel 群 G の位数有限の元全体は部分群を作る. この部分群を G の**ねじれの群**という. 有限生成加群が定理 3.4 におけるような構造をもつとき, そのねじれの群は $\boldsymbol{Z}_{e_1}\oplus\boldsymbol{Z}_{e_2}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}$ と同型である.

つぎの系は定理 3.4 から明らかである.

系　G を有限生成加群とするとき, つぎが成り立つ.

(i)　G はねじれの群と自由加群の直和と同型である.

(ii)　G のねじれの群が単位群ならば, G は自由加群である.

問 3.5　系は定理 3.4 を用いず, 直接に証明することができる. これを試みよ. (単因子論を使わない.)

定理 3.5　有限生成加群 G が定理 3.4 におけるような構造をもつとき, $r, s, e_1, e_2, \cdots, e_r$ は G によって一意的に定まる.

証明
$$G \simeq \boldsymbol{Z}_{e_1}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}\oplus\boldsymbol{Z}^s \qquad (1<e_1\,|\,e_2\,|\cdots|\,e_r,\ s\geqq 0),$$
$$\simeq \boldsymbol{Z}_{e_1'}\oplus\cdots\oplus\boldsymbol{Z}_{e_{r'}'}\oplus\boldsymbol{Z}^{s'} \qquad (1<e_1'\,|\,e_2'\,|\cdots|\,e_{r'}',\ s'\geqq 0)$$

のとき, $r=r'$, $s=s'$, $e_i=e_i'$ $(1\leqq i\leqq r)$ をいわねばならない. T を G のねじれの群とすると

(＊) $$G/T \simeq \boldsymbol{Z}^s \simeq \boldsymbol{Z}^{s'},$$

(＊＊) $$T \simeq \boldsymbol{Z}_{e_1}\oplus\cdots\oplus\boldsymbol{Z}_{e_r} \simeq \boldsymbol{Z}_{e_1'}\oplus\cdots\oplus\boldsymbol{Z}_{e_{r'}'}$$

である．(＊)から $s=s'$ を得る(自由加群の階数の一意性!)．つぎに $r=r'$ を示そう．$r\geqq r'$ としてよい．e_1 を割る素数 p をとる．$T_p=\{x\in T\mid px=0\}$ とおくと T_p は T の部分群である．$T\simeq\boldsymbol{Z}_{e_1}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}$ $(e_1\,|\,e_2\,|\cdots|\,e_r)$ より，$|T_p|=p^r$ である．一方，$T\simeq\boldsymbol{Z}_{e_1'}\oplus\cdots\oplus\boldsymbol{Z}_{e_{r'}'}$ より $|T_p|\leqq p^{r'}$．したがって $r=r'$ でなければならない．最後に $e_1=e_1', \cdots, e_{i-1}=e_{i-1}'$ として，$e_i=e_i'$ を示そう．$T_{e_i}=\{x\in T\mid e_ix=0\}$ とおくと，T_{e_i} は T の部分群である．$T\simeq\boldsymbol{Z}_{e_1}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}$ $(e_1\,|\,e_2\,|\cdots|\,e_r)$ より $|T_{e_i}|=e_1e_2\cdots e_{i-1}e_i^{\,r-i+1}$ である．一方，$j\geqq i$ に対して e_i と e_j' の最大公約数を d_j とすると，$T\simeq\boldsymbol{Z}_{e_1'}\oplus\cdots\oplus\boldsymbol{Z}_{e_r'}$ $(e_1'\,|\,e_2'\,|\cdots|\,e_r',\ e_k=e_k'\,(1\leqq k\leqq i-1))$ により $|T_{e_i}|=e_1e_2\cdots e_{i-1}d_id_{i+1}\cdots d_r$．したがって，$e_i^{\,r-i+1}=d_id_{i+1}\cdots d_r$, $d_j\leqq e_j\,(j\geqq i)$ を得る．これから，$e_i=d_j\ (j\geqq i)$ がわかる．とくに $e_i=d_i$ で，これは $e_i=e_i'$ を示す．▌

$$G \simeq \boldsymbol{Z}_{e_1}\oplus\cdots\oplus\boldsymbol{Z}_{e_r}\oplus\boldsymbol{Z}^s \qquad (e_1\,|\,e_2\,|\cdots|\,e_r,\ \ e_i>1,\ \ s\geqq 0)$$

のとき，整数の組

$$(e_1, e_2, \cdots, e_r, \underbrace{0, \cdots, 0}_{s})$$

を有限生成加群 G の**不変系**という．定理3.5によれば，二つの有限生成加群が同型であるためには，不変系が一致することが必要十分である．或る素数 p に対して不変系が $(\underbrace{p, p, \cdots, p}_{n})$ なる有限生成 Abel 群を $((\underbrace{p, p, \cdots, p}_{n})$ 型の$)$ **基本 Abel 群**という．

最後に環 $\boldsymbol{Z}_{p^e}=\boldsymbol{Z}/\langle p^e\rangle$ $(e\geqq 1,\ p$ は素数$)$ の乗法群 $\boldsymbol{Z}_{p^e}{}^*$ の不変系を調べてみよう．

例題 3.2 (i) p が奇素数ならば，$\boldsymbol{Z}_{p^e}{}^*$ は巡回群である．したがってその不変系は $(p^{e-1}(p-1))$ である．(ii) $p=2$ ならば，$\boldsymbol{Z}_{2^e}{}^*$ の不変系は $(2, 2^{e-2})$ である．ただし $e\geqq 3$ とする．$e=1, 2$ のときはそれぞれ位数 1, 2 の巡回群である．——

証明にはつぎの補題を用いる．

補題 3.4 p が奇素数のとき

(＊) $$(p+1)^{p^{n-1}} = 1+kp^n, \qquad (k, p) = 1$$

である．また $n\geqq 3$ のとき

(＊＊) $$5^{2^{n-2}} = 1+k2^n, \qquad (k, 2) = 1, \qquad 5^{2^{n-3}} \not\equiv -1 \pmod{2^n}$$

である. ——

この補題の証明は2項定理と n に関する数学的帰納法を用いて容易に証明できるから，読者にまかせる.

[例題 3.2 の証明] $p\neq 2$ の場合: $\boldsymbol{Z}_p=\boldsymbol{Z}/\langle p\rangle$ は体であるからその乗法群 $\boldsymbol{Z}_p{}^*$ は位数 $p-1$ の巡回群である(定理 1.10). $\boldsymbol{Z}_{p^e}{}^*$ から $\boldsymbol{Z}_p{}^*$ の上への自然な準同型があるから，$\boldsymbol{Z}_{p^e}{}^*$ は位数 $p-1$ の元を含む. 一方，補題 3.4 の(＊)は，$p+1$ が $\boldsymbol{Z}_{p^e}{}^*$ において位数 p^{e-1} であることを示す. したがって $\boldsymbol{Z}_{p^e}{}^*$ は位数 $p-1$ の元 x と位数 p^{e-1} の元 y を含む. x と y の位数は互いに素だから xy の位数は $p^{e-1}\cdot(p-1)$ である. したがって $|\boldsymbol{Z}_{p^e}{}^*|=p^{e-1}(p-1)$ であるから $\boldsymbol{Z}_{p^e}{}^*$ は巡回群である.

$p=2$ の場合: 補題 3.4 の(＊＊)は $\boldsymbol{Z}_{2^e}{}^*\,(e\geqq 3)$ において5は位数 2^{e-2} であることおよび5で生成される $\boldsymbol{Z}_{2^e}{}^*$ の部分群は -1 を含まないことを示している. 5, -1 で生成される $\boldsymbol{Z}_{2^e}{}^*$ の部分群をそれぞれ H, K とすると，$H\cap K=1$ だから，HK と $\boldsymbol{Z}_{2^e}{}^*$ の位数を比べて $\boldsymbol{Z}_{2^e}{}^*=HK$ を得る. $H\cap K=1$ より $HK\simeq H\otimes K$, $H\simeq\boldsymbol{Z}_{2^{e-2}}$, $K\simeq\boldsymbol{Z}_2$ だから

$$\boldsymbol{Z}_{2^e}{}^*\simeq\boldsymbol{Z}_2\otimes\boldsymbol{Z}_{2^{e-2}}$$

を得る. ▌

§3.4 主イデアル整域上の単因子論

§3.1-§3.3 の結果のほとんどすべては，主イデアル整域上の単因子論や有限生成加群に対して一般化される. 本節と次節でその概要を説明するが，それは主イデアル整域と任意の環の上の加群の概念の説明がほとんどである. これらの概念が確立されれば，§3.1-§3.3 の議論は一部を除いてそのまま適用できるから，修正しなければならない点について注意するにとどめるであろう.

可換環 $\mathfrak{R}$ は

(3.5) $$ab=0\quad(a,b\in\mathfrak{R})\Longrightarrow a=0\ \text{ または }\ b=0$$

なる条件を満たすとき，**整域**とよばれる.

$\mathfrak{R}$ を整域とする. $\mathfrak{R}\ni a,b$ に対して $a=bc$ なる $c\in\mathfrak{R}$ が存在するとき，a は b で割れるといい，$b\,|\,a$ と書く. 容易にわかるように

(3.6) $$b\,|\,a\Longleftrightarrow\langle b\rangle\supseteqq\langle a\rangle$$

である. ここで $\langle a\rangle$ は a で生成される $\mathfrak{R}$ の主イデアルを表わす. $\mathfrak{R}\ni p$ は,

(3.7)　　$p = ab \quad (a, b \in \mathfrak{R}) \Longrightarrow a \in \mathfrak{R}^*$ または $b \in \mathfrak{R}^*$

であるとき**素元**といわれる．$\mathfrak{R}^*$ は $\mathfrak{R}$ の単元全体の集合である．また

(3.8)　　$\mathfrak{R}^* \not\ni a \neq 0 \Longrightarrow \langle a \rangle \supsetneqq \langle a^2 \rangle$

が成り立つ．

問 3.6　(3.6), (3.8) を証明せよ．——

整域 $\mathfrak{R}$ のすべてのイデアルが主イデアルであるとき，すなわち $\mathfrak{R}$ の任意のイデアル $\mathfrak{A}$ が $\mathfrak{A} = \langle a \rangle$ $(a \in \mathfrak{R})$ と書けるとき，$\mathfrak{R}$ を**主イデアル整域**という．整数環 $\boldsymbol{Z}$ や体 k 上の多項式環 $k[X]$ は主イデアル整域である．

主イデアル整域 $\mathfrak{R}$ の元 $a_1, a_2, \cdots, a_n$ に対して

$$\langle a_1, a_2, \cdots, a_n \rangle = \langle d \rangle$$

なる d を $a_1, a_2, \cdots, a_n$ の**最大公約元**という．このとき

(3.9)　$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ が $\mathfrak{R}$ において解をもつためには $d|b$ なることが必要十分である．

問 3.7　(3.9) を証明せよ．また $a, b \in \mathfrak{R}$ が互いに素（すなわち最大公約元が 1）のとき，$\mathfrak{R}/\langle ab \rangle \simeq \mathfrak{R}/\langle a \rangle \oplus R/\langle b \rangle$ を示せ．——

つぎの補題は，主イデアル整域の取り扱いにおいて基本的である．

補題 3.5　主イデアル整域 $\mathfrak{R}$ のイデアルからなる任意の集合は（包含関係に関して）極大元をもつ．——

この補題の証明は，集合論における Zorn の補題の簡単な応用なのであるが，もう少し一般の環に対して成り立つ或る命題（§4.3 定理 4.8 参照）の特別な場合でもあるので，その証明は（Zorn の補題の説明とともに）第 4 章で述べるであろう．

補題 3.5 の応用として主イデアル整域における素元分解とその一意性を示そう．主イデアル整域 $\mathfrak{R}$ の $\mathfrak{R}$ 自身と異なるイデアル全体の集合は，補題 3.5 により極大元をもつ．すなわち $\mathfrak{R}$ に極大イデアル——“$\mathfrak{A} \subseteqq \mathfrak{B},\ \mathfrak{B} \neq \mathfrak{R} \Longrightarrow \mathfrak{A} = \mathfrak{B}$” なるイデアル $\mathfrak{A}$——が存在する．

$$\mathfrak{P} = \{\mathfrak{p}_\lambda \mid \lambda \in \Lambda\}$$

を $\mathfrak{R}$ の極大イデアル全体の集合としよう．$\mathfrak{p}_\lambda = \langle p_\lambda \rangle$ とおくと，p_λ は $\mathfrak{R}$ の素元である．実際，

$$p_\lambda = ab,\ a \notin \mathfrak{R}^*,\ b \notin \mathfrak{R}^* \Longrightarrow \langle p_\lambda \rangle \subseteqq \langle a \rangle,\ \langle p_\lambda \rangle \subseteqq \langle b \rangle \qquad ((3.6) による)$$

$$\Longrightarrow \langle p_\lambda \rangle = \langle a \rangle = \langle b \rangle \qquad (\langle p_\lambda \rangle \text{ の極大性})$$
$$\Longrightarrow \langle p_\lambda \rangle = \langle p_\lambda{}^2 \rangle$$

となり，(3.8)に矛盾する.

$$\boldsymbol{P} = \{p_\lambda \mid \lambda \in \Lambda\}$$

とおく．p_λ は $\mathfrak{p}_\lambda$ に対して一意的に定まるものではないが $\mathfrak{p}_\lambda$ に対して一つ選んで固定しておく．ここでつぎのことに注意しておく：

(＊) $\qquad p_\lambda \mid ab \quad (p_\lambda \in \boldsymbol{P},\ a, b \in \mathfrak{R}) \Longrightarrow p_\lambda \mid a$ または $p_\lambda \mid b$.

実際，$p_\lambda \nmid a$ とすると $\langle p_\lambda \rangle$ の極大性により $\langle p_\lambda, a \rangle = \mathfrak{R}$，すなわち p_λ と a は互いに素である．よって(3.9)により $p_\lambda x + ay = 1$ なる $x, y \in \mathfrak{R}$ が存在する．したがって $b = p_\lambda bx + aby$，$p_\lambda \mid ab$ より $p_\lambda \mid b$ を得る.

定理 3.6 $\mathfrak{R}$ を主イデアル整域とする．$\mathfrak{R} \ni a \neq 0$ とすると，

(3.10) $$a = u \prod_\lambda{}' p_\lambda{}^{e_\lambda} \qquad (u \in \mathfrak{R}^*,\ 0 \leqq e_\lambda \in \boldsymbol{Z})$$

と書け，e_λ は a によって一意的に定まる．ここで $\prod'$ は有限個の λ を除いて $e_\lambda = 0$ となる積を表わす.

証明 最初に $\mathfrak{R} \ni a \neq 0$ が(3.10)の形に書けることを示そう.

$$X = \left\{ \langle b \rangle \,\middle|\, b \mid a,\ a = b \prod_{\lambda \in \Lambda}{}' p_\lambda{}^{e_\lambda} \right\}$$

とおく．$X \ni \langle a \rangle$ であるから X は空集合ではない．補題 3.5 により X は極大元 $\langle u \rangle$ をもつ．$\langle u \rangle = \mathfrak{R}$ を示せばよいから，$\langle u \rangle \neq \mathfrak{R}$ と仮定して矛盾をだす．$X \ni \langle u \rangle$ より $a = u \prod_\lambda{}' p_\lambda{}^{e_\lambda}$ である．$\langle u \rangle$ を含む $\mathfrak{R}$ の極大イデアル $\langle p \rangle$ ($p \in \boldsymbol{P}$) をとると(補題 3.5 !)，$u = pu'$ で $\langle u \rangle \subsetneqq \langle u' \rangle$ である．このとき $a = u'p \prod_\lambda{}' p_\lambda{}^{e_\lambda}$ であるから $\langle u' \rangle \in X$ となり，これは $\langle u \rangle$ の極大性に反する．つぎに一意性を示そう.

$$a = u \prod_\lambda{}' p_\lambda{}^{e_\lambda} = u' \prod_\lambda{}' p_\lambda{}^{f_\lambda} \qquad (u, u' \in \mathfrak{R}^*,\ 0 \leqq e_\lambda, f_\lambda \in \boldsymbol{Z})$$

とする．或る μ に対して $e_\mu > f_\mu$ とすると

$$p_\mu \mid u p_\mu{}^{e_\mu - f_\mu} \prod_{\lambda \neq \mu}{}' p_\lambda{}^{e_\lambda} = u' \prod_{\lambda \neq \mu}{}' p_\lambda{}^{f_\lambda}$$

であるが，この式の第1項と第3項を見比べて，上の(＊)を用いれば，或る $\nu \in \Lambda$ ($\nu \neq \mu$) に対して $p_\mu \mid p_\nu$ でなければならない．これは $p_\mu = p_\nu$ を示すから矛盾である. ▌

つぎに §3.1 の定理 3.1 を主イデアル整域の場合に一般化しよう．ただし証明

は一部修正する必要がある.

$\mathfrak{R}$ を主イデアル整域, $M_{m,n}(\mathfrak{R})$ を $\mathfrak{R}$ の元を成分とする m 行 n 列の行列全体の集合とする. $M_{m,n}(\mathfrak{R}) \ni A, B$ に対して, $X \in GL_m(\mathfrak{R})$, $Y \in GL_n(\mathfrak{R})$ が存在して

$$XAY = B \tag{3.11}$$

なる関係は, $M_{m,n}(\mathfrak{R})$ の上の同値関係である.

定理 3.7　同値関係 (3.11) の各同値類は,

$$\begin{bmatrix} e_1 & & & & & & \\ & e_2 & & & & & \\ & & \ddots & & & & \\ & & & e_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix} \qquad (e_1 \mid e_2 \mid \cdots \mid e_r,\ \ e_r \neq 0) \tag{3.12}$$

なる形の行列を含む. さらにイデアル $\langle e_1\rangle, \langle e_2\rangle, \cdots, \langle e_r\rangle$ はその同値類によって一意的に定まる.

証明　Ω を一つの同値類としよう. Ω の行列に

(i)　或る二つの行を入れかえる,

(ii)　或る行に他の行の何倍かを加える,

(i)′　或る二つの列を入れかえる,

(ii)′　或る列に他の列の何倍かを加える

なる四つの操作をほどこして得られる行列は, やはり Ω に含まれる. Ω の行列の成分として現われる $\mathfrak{R}$ の 0 でない元全体を X' として,

$$X = \{\langle x\rangle \mid x \in X'\}$$

とおく. 補題 3.5 により X は極大元 $\langle e_1\rangle$ をもつ. $\Omega \ni A$ を, e_1 を成分とする行列として, 必要ならば (i), (i)′ を A にほどこして, e_1 が A の $(1,1)$ 成分にあるとしてよい:

$$A = \begin{bmatrix} e_1 & a_{12} & \cdots & a_{1n} \\ a_{21} & & & \\ \vdots & & * & \\ a_{m1} & & & \end{bmatrix}.$$

このとき $e_1 | a_{1j}$ $(j \geqq 2)$, $e_1 | a_{i1}$ $(i \geqq 2)$ を示そう. e_1 と a_{1j} の最大公約元を d とすると, (3.9) により $e_1x + a_{1j}y = d$ なる $x, y \in \mathfrak{R}$ が存在する. Y をつぎの形の行列とする:

$$Y = \begin{bmatrix} x & \cdots & -e_1/d & & & \\ \vdots & 1 & \vdots & & & \\ \vdots & & \ddots & \vdots & & \\ \vdots & & 1 & \vdots & & \\ y & \cdots\cdots & a_{1j}/d & \cdots\cdots\cdots & & \\ & & \vdots & 1 & & \\ & & \vdots & & \ddots & \\ & & \vdots & & & 1 \end{bmatrix}_j .$$

(上の $-e_1/d$ は第 j 列, a_{1j}/d の行は第 j 行)

このとき $Y \in GL_n(\mathfrak{R})$, $AY \in \Omega$ で

$$AY = \begin{bmatrix} d & * & \cdots & * \\ * & & & \\ \vdots & & * & \\ * & & & \end{bmatrix}$$

となる. $X \ni \langle d \rangle \supseteqq \langle e_1 \rangle$ であるから $\langle e_1 \rangle$ の極大性により $\langle d \rangle = \langle e_1 \rangle$. これは $e_1 | a_{1j}$ を示す. 同様にして $e_1 | a_{i1}$ $(i \geqq 2)$ が示される. これからあとは, 定理3.1の証明をそのまま真似をすれば, Ω が (3.12) の形の行列を含むことがわかる. また $\langle e_1 \rangle, \langle e_2 \rangle, \cdots, \langle e_r \rangle$ の一意性の証明は, 定理3.1のそれを何等修正することなく通用する. くわしくは読者自ら確かめられたい. ▌

なお上の証明から $GL_n(\mathfrak{R})$ の生成系についてつぎの定理が得られる.

定理 3.8 $GL_n(\mathfrak{R})$ ($\mathfrak{R}$ は主イデアル整域) は,

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ \cdots\cdots & & a & \cdots & b & \cdots\cdots & \\ & & \vdots & \ddots & \vdots & & \\ \cdots\cdots & & c & \cdots & d & \cdots\cdots & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathfrak{R})$$

(上の a, c は第 i 列, b, d は第 j 列; a, b の行は第 i 行, c, d の行は第 j 行)

の形の行列で生成される．($n=2$ のときは何もいっていない！)

§3.5 $\mathfrak{R}$ 加群

つぎに進むために，任意の環 $\mathfrak{R}$ に対して $\mathfrak{R}$ 加群の概念を導入しよう．これは $\mathfrak{R}$ が斜体のときは，線型空間の概念にほかならないのであるが，$\mathfrak{R}$ が斜体でないときは $\mathfrak{R}$ 加群の取り扱いは線型空間のときほど簡単ではない．

集合 V が環 $\mathfrak{R}$ 上の加群——$\mathfrak{R}$ **加群**——であるとは，

I　V は加群である，

II　$\mathfrak{R}\times V$ から V への写像

$$\mathfrak{R}\times V \ni (\alpha, v) \longmapsto \alpha v \in V$$

が定義されていて

$$\alpha(\beta v) = (\alpha\beta)v \qquad (\alpha, \beta \in \mathfrak{R},\ v \in V),$$

$$1v = v \qquad (v \in V,\ 1 \text{ は } \mathfrak{R} \text{ の乗法の単位元}),$$

III
$$\left.\begin{aligned} \alpha(u+v) &= \alpha u+\alpha v, \\ (\alpha+\beta)u &= \alpha u+\beta u \end{aligned}\right. \quad (\alpha, \beta \in \mathfrak{R},\ u, v \in V)$$

なる公理を満たすもののことである．とくに $\mathfrak{R}$ が斜体のとき，V は $\mathfrak{R}$ 上の線型空間である．

上で定義したのは，正確には**左** $\mathfrak{R}$ **加群**とよばれるものである．同じように右 $\mathfrak{R}$ 加群が定義される．すなわち II, III の代りに，

II′　$V\times\mathfrak{R}$ から V への写像

$$(v, \alpha) \longmapsto v\alpha$$

が定義されていて

$$v(\alpha\beta) = (v\alpha)\beta \qquad (v \in V,\ \alpha, \beta \in \mathfrak{R}),$$

$$v1 = v,$$

III′
$$\left.\begin{aligned} (u+v)\alpha &= u\alpha+v\alpha, \\ u(\alpha+\beta) &= u\alpha+u\beta \end{aligned}\right. \quad (\alpha, \beta \in \mathfrak{R},\ u, v \in V)$$

なる条件を満たすとき，V を**右** $\mathfrak{R}$ **加群**という．一般には(とくに $\mathfrak{R}$ が非可換環のとき)左右の $\mathfrak{R}$ 加群を区別しなければならないことも起るが，概念の構成はまったく平行なので，本節では左 $\mathfrak{R}$ 加群の場合のみを述べ，左 $\mathfrak{R}$ 加群を単に $\mathfrak{R}$ 加群という．

例 3.1　(i)　V を任意の加群とすると V は $\boldsymbol{Z}$ 加群である．$\boldsymbol{Z}\ni n$, $V\ni v$ に対して $nv=\underbrace{v+\cdots+v}_{n}$ とすれば，明らかに上のすべての公理 I–III が満たされる．

(ii)　$\mathfrak{R}$ を任意の環とする．$\mathfrak{R}^n$ を $\mathfrak{R}$ の n 個の直積集合として，それを自然に加群とみなす．$\mathfrak{R}\ni\alpha$, $\mathfrak{R}^n\ni x=(x_1, x_2, \cdots, x_n)$ に対して

$$\alpha x=(\alpha x_1, \alpha x_2, \cdots, \alpha x_n)$$

とおけば，$\mathfrak{R}^n$ は $\mathfrak{R}$ 加群となる．とくに $\mathfrak{R}$ 自身は $\mathfrak{R}$ 加群である．また $\mathfrak{R}$ の左イデアルは自然に左 $\mathfrak{R}$ 加群とみなせる．——

V を $\mathfrak{R}$ 加群とする．V の部分加群 U は

$$U\ni u, \quad \mathfrak{R}\ni\alpha \Longrightarrow U\ni\alpha u$$

なる条件を満たすとき，V の $\mathfrak{R}$ **部分加群**という．$\mathfrak{R}$ を $\mathfrak{R}$ 加群と見れば，$\mathfrak{R}$ の $\mathfrak{R}$ 部分加群とは左イデアルのことにほかならない．V の部分集合 S に対して

$$\langle S\rangle=\{\alpha_1 s_1+\cdots+\alpha_n s_n \mid \alpha_i\in\mathfrak{R},\ s_i\in S\}$$

とおけば，$\langle S\rangle$ は V の $\mathfrak{R}$ 部分加群となる．$\langle S\rangle$ を S で生成された $\mathfrak{R}$ 部分加群という．とくに $V=\langle S\rangle$ のとき，S を V の**生成系**，S の元を**生成元**という．有限個の元からなる生成系が存在するとき，V は**有限生成**であるといわれる．

U を V の $\mathfrak{R}$ 部分加群とするとき，剰余群 V/U は自然に $\mathfrak{R}$ 加群となる．すなわち $\bar{v}$ で $v\in V$ を含む U の剰余類を表わせば，

$$\alpha\bar{v}=\overline{\alpha v} \qquad (\alpha\in\mathfrak{R},\ v\in V)$$

とおくことにより V/U は $\mathfrak{R}$ 加群となる．

$\mathfrak{R}$ 加群 V, V' に対して，V から V' への写像 f が

$$\left.\begin{aligned} f(u+v)&=f(u)+f(v),\\ f(\alpha v)&=\alpha f(v)\end{aligned}\right. \qquad (u, v\in V,\ \alpha\in\mathfrak{R})$$

なる条件を満たすとき，V から V' への $\mathfrak{R}$ **準同型**という．V から V' の上への $\mathfrak{R}$ **同型**（$\mathfrak{R}$ 準同型で全単射なるもの）が存在するとき，V と V' は同型であるといい，

$$V\underset{\mathfrak{R}}{\simeq}V' \quad \text{あるいは簡単に} \quad V\simeq V'$$

と書く．

問 3.8　f を $\mathfrak{R}$ 加群 V から $\mathfrak{R}$ 加群 V' の上への $\mathfrak{R}$ 準同型とすれば，$V/f^{-1}(0')\underset{\mathfrak{R}}{\simeq}V'$（$0'$ は V' の零元）を示せ．

問 3.9　$\mathfrak{R}$ 加群 V に対して $\mathfrak{N}(V)=\{\alpha\in\mathfrak{R}\mid \alpha v=0\ (\forall v\in V)\}$ とおく．このときつぎの (i), (ii) を示せ：

(i) $\mathfrak{N}(V)$ は $\mathfrak{R}$ の左イデアルである．(ii) $\mathfrak{A},\mathfrak{B}$ を $\mathfrak{R}$ の左イデアルとするとき，$\mathfrak{N}(\mathfrak{R}/\mathfrak{A})=\mathfrak{A}$．また $\mathfrak{R}/\mathfrak{A}\simeq\mathfrak{R}/\mathfrak{B}\Longrightarrow\mathfrak{A}=\mathfrak{B}$．——

$\mathfrak{R}$ 加群 V はつぎの性質を満たす生成系 S をもつとき，$\mathfrak{R}$ **自由加群**という：S の異なる有限個の任意の元 $s_1, s_2, \cdots, s_n$ に対して

$$\alpha_1 s_1+\alpha_2 s_2+\cdots+\alpha_n s_n = 0\ \ (\alpha_i\in\mathfrak{R}) \Longrightarrow \alpha_1=\alpha_2=\cdots=\alpha_n=0.$$

このとき V の各元は

$$\sum_{s\in S}\alpha_s s \qquad (\text{有限和})$$

の形に一意的に書ける．このような S を $\mathfrak{R}$ 自由加群 V の**基底**という．基底 S は一般には無限集合かもしれないが，$\mathfrak{R}$ 自由加群 V が有限生成ならば，基底 S も有限集合でなければならない．このとき S に含まれる元の数 $|S|$ を V の**階数**という．

注意　一般には有限生成 $\mathfrak{R}$ 自由加群 V の階数が，V に対して一意的に定まるかどうかは分らない．しかし $\mathfrak{R}$ が可換環のときは，§3.2 で $\boldsymbol{Z}$ に対して述べたのとまったく同様にして階数の一意性が証明される．また $\mathfrak{R}$ が斜体のときも階数の一意性が成り立つことは，第1章 §1.7 で述べた．さらに $\mathfrak{R}$ が斜体ならば，任意の $\mathfrak{R}$ 加群は $\mathfrak{R}$ 自由加群 (階数は無限かもしれない) であることが Zorn の補題を用いて証明される．これが斜体上の加群の取り扱いが簡単になる理由である．

問 3.10　$\mathfrak{R}$ が斜体でないとき，自由加群でない $\mathfrak{R}$ 加群が存在することを示せ．——

§3.2 の補題 3.3 はそのままの形で $\mathfrak{R}$ 自由加群に対して成り立つ．

補題 3.6　V を階数 n の $\mathfrak{R}$ 自由加群，$v_1, v_2, \cdots, v_n$ をその基底とする．

(i)　U を n 個の元からなる生成系をもつ任意の $\mathfrak{R}$ 加群とすると V から U の上への $\mathfrak{R}$ 準同型が存在する．もっとくわしく $U=\langle u_1, u_2, \cdots, u_n\rangle$ ならば，V から U の上への $\mathfrak{R}$ 準同型 f で $f(v_i)=u_i$ なるものが存在する．

(ii)　U を任意の $\mathfrak{R}$ 加群とし，φ を U から V の上への $\mathfrak{R}$ 準同型とする．$f^{-1}(0)=N$ とおくと，U の $\mathfrak{R}$ 部分加群 H が存在して

$$U=N+H,\qquad N\cap H=\{0\},\qquad H\simeq V$$

となる．

問 3.11　補題3.6を確かめよ. ——

主イデアル整域上の有限生成加群に対して§3.2–§3.3の主要定理は，すべてそのままの形で成り立つ(定理3.9–3.12). その証明も最後の定理3.12を除けば，§3.2–§3.3の対応する定理の証明をそのまま真似をすればよいから，復習をかねて読者自ら確かめられたい. 以下 $\mathfrak{R}$ は主イデアル整域とする.

定理 3.9　V を階数 n の $\mathfrak{R}$ 自由加群，U をその $\mathfrak{R}$ 部分加群とすれば，U は階数が高々 n の $\mathfrak{R}$ 自由加群である.

定理 3.10　V を階数 n の $\mathfrak{R}$ 自由加群，U をその $\mathfrak{R}$ 部分加群とすれば，V の基底 $v_1, v_2, \cdots, v_n$ を適当にとり

$$e_1v_1,\ e_2v_2,\ \cdots,\ e_rv_r \qquad (e_1|e_2|\cdots|e_r,\ r\leqq n)$$

が U の基底になるようにできる.

定理 3.11　V を有限生成 $\mathfrak{R}$ 加群とすれば，$\mathfrak{R}\ni e_1, e_2, \cdots, e_r$ と整数 s が存在して

$$e_1|e_2|\cdots|e_r \qquad (e_i\neq 0,\ R\neq\langle e_i\rangle),$$

$$V\simeq \mathfrak{R}/\langle e_1\rangle\oplus\mathfrak{R}/\langle e_2\rangle\oplus\cdots\oplus\mathfrak{R}/\langle e_r\rangle\oplus\mathfrak{R}^s.$$

定理 3.12　定理3.11において，s およびイデアル $\langle e_1\rangle, \langle e_2\rangle, \cdots, \langle e_r\rangle$ は V によって一意的に定まる. ——

一般に $\mathfrak{R}$ 加群 V に対して

$$V_0 = \{v\in V \mid \alpha v=0\ (0\neq\exists\alpha\in\mathfrak{R})\}$$

とおけば，V_0 は V の $\mathfrak{R}$ 部分加群となる. これを V の**ねじれの $\mathfrak{R}$ 部分加群**という. 主イデアル整域 $\mathfrak{R}$ 上の有限生成加群 V が定理3.11におけるような構造をもっているとき，V のねじれの $\mathfrak{R}$ 部分加群 V_0 は $\mathfrak{R}/\langle e_1\rangle\oplus\cdots\oplus\mathfrak{R}/\langle e_r\rangle$ と同型であり，

$$V/V_0\simeq\mathfrak{R}^s$$

となる. これから s が V に対して一意的に定まることがわかる(可換環上の自由加群の階数の一意性). したがって定理3.12を証明するには

$$(3.13)\qquad V\simeq\mathfrak{R}/\langle e_1\rangle\oplus\cdots\oplus\mathfrak{R}/\langle e_r\rangle \qquad (e_1|e_2|\cdots|e_r,\ e_i\neq 0,\ \mathfrak{R}\neq\langle e_i\rangle)$$

のとき，イデアル $\langle e_1\rangle, \langle e_2\rangle, \cdots, \langle e_r\rangle$ の一意性をいえばよい. ところで $\mathfrak{R}\ni a$ の素元分解を

$$a = up_1^{a_1}p_2^{a_2}\cdots p_t^{a_t} \qquad (u\in\mathfrak{R}^*,\ 0<a_i\in \boldsymbol{Z})$$

とするとき，問 3.7 により，

$$\mathfrak{R}/\langle a\rangle \simeq \mathfrak{R}/\langle p_1^{a_1}\rangle \oplus\cdots\oplus \mathfrak{R}/\langle p_t^{a_t}\rangle \tag{3.14}$$

である．(3.13) の右辺の各項に (3.14) を適用すれば，

$$V \simeq \mathfrak{R}/\langle p_1^{b_1}\rangle \oplus \mathfrak{R}/\langle p_2^{b_2}\rangle \oplus\cdots\oplus \mathfrak{R}/\langle p_u^{b_u}\rangle \qquad (0<b_i\in \boldsymbol{Z})^{1)} \tag{3.15}$$

の形となる．(3.15) における $\langle p_i^{b_i}\rangle$ の一意性がいえれば，$e_1|e_2|\cdots|e_r$ なる条件によって，$\langle e_1\rangle, \langle e_2\rangle, \cdots, \langle e_r\rangle$ の一意性が容易にわかる．ところで (3.15) における $\langle p_i^{b_i}\rangle$ の一意性は，いまここで証明することもできるが，それはつぎの章で証明される Krull-Remak-Schmidt の定理から直ちに得られるので次章にゆずることにしよう．

最後に定理 3.11，3.12 の応用として，線型代数における 'Jordan の標準形' の問題をとりあげよう．

例題 3.3 V を複素数体 $\boldsymbol{C}$ [2] 上の n 次元線型空間，T を V の線型変換とする．V の基底を適当にとれば，T に対応する行列が

$$\begin{bmatrix} J(\alpha_1, k_1) & & & \\ & J(\alpha_2, k_2) & & \\ & & \ddots & \\ & & & J(\alpha_r, k_r) \end{bmatrix}, \qquad J(\alpha, k) = \underbrace{\begin{bmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \alpha \end{bmatrix}}_{k} \Big\} k \tag{3.16}$$

の形となる．$\alpha_1, \alpha_2, \cdots, \alpha_r$, $k_1, k_2, \cdots, k_r$ は T によって一意的に定まる．

［証明］ $\mathfrak{R}$ を $\boldsymbol{C}$ 上の多項式環 $\boldsymbol{C}[X]$ とする：$\mathfrak{R}=\boldsymbol{C}[X]$．$\mathfrak{R}$ は主イデアル整域である (問 1.62)．V をつぎのようにして $\mathfrak{R}$ 加群とみなすことができる：

$\boldsymbol{C}[X] \ni f(X)=a_0+a_1X+\cdots+a_mX^m$ に対して

$$f(X)v = a_0v+a_1T(v)+\cdots+a_mT^m(v) \qquad (v\in V)$$

とおけば，これは $\mathfrak{R}$ 加群の公理 I, II, III を満たすことが容易に験証される．

まずつぎのことに注意する：

(α) V の任意の元 $v\neq 0$ に対して，或る $f(X)\in \boldsymbol{C}[X]$ が存在して，$f(X)v=0$．実際，$n+1$ 個のベクトル $v, T(v), T^2(v), \cdots, T^n(v)$ は線型従属だから，

---

1) $p_1, p_2, \cdots, p_u$ が互いに異なるとは限らない．

2) 任意の代数閉体でよい．体 k は，k 上の任意の多項式 $f(X)$ $(\deg f\geqq 1)$ に対して，$f(X)=0$ が k に根をもつとき代数閉体といわれる．

$$a_0v+a_1T(v)+\cdots+a_nT^n(v)=0$$

なる $a_0, a_1, \cdots, a_n \in \boldsymbol{C}$ が存在する．これは $(a_0+a_1X+\cdots+a_nX^n)v=0$ を示す．

さて，V は $\boldsymbol{C}$ 上有限次元だから当然有限生成 $\mathfrak{R}$ 加群である．$\boldsymbol{C}[X]$ の素元は 1 次式 $X-\alpha$ $(\alpha \in \boldsymbol{C})$ にほかならないから，定理 3.12 と (3.15) により，

$$V \simeq \mathfrak{R}/\langle(X-\alpha_1)^{b_1}\rangle \oplus\cdots\oplus \mathfrak{R}/\langle(X-\alpha_u)^{b_u}\rangle \oplus \mathfrak{R}^s \qquad (0<b_i \in \boldsymbol{Z})$$

となるが，(α) から $s=0$ がわかる．したがって

$$V = V_1 \oplus V_2 \oplus\cdots\oplus V_u, \qquad V_i \simeq \mathfrak{R}/\langle(X-\alpha_i)^{b_i}\rangle \quad (i=1,2,\cdots,u)$$

となる．$\mathfrak{R}$ 同型 $V_i \simeq \mathfrak{R}/\langle(X-\alpha_i)^{b_i}\rangle$ において，$\mathfrak{R}$ の単位元 1 に対応する V_i の元を v_i とすれば，V_i の任意の元は，

$$f(X)v_i \qquad (\deg f<b_i)$$

の形に書ける．$v_{ij}=(X-\alpha_i)^j v_i$ $(0 \leqq j \leqq b_i-1)$ とおけば，$v_{i0}, v_{i1}, \cdots, v_{i,b_i-1}$ が V_i の基底である．実際，$f(X)=a_0+a_1(X-\alpha_i)+\cdots+a_{b_i-1}(X-\alpha_i)^{b_i-1}$ と書けば，

$$f(X)v_i = a_0v_{i0}+a_1v_{i1}+\cdots+a_{b_i-1}v_{i,b_i-1}$$

となり $V_i=\langle v_{i0}, \cdots, v_{i,b_i-1}\rangle$ である．さらに $0 \leqq \deg f<b_i$ のとき $f(X)v_i \neq 0$ であるから，$v_{i0}, v_{i1}, \cdots, v_{i,b_i-1}$ は線型独立である．ところで，$(X-\alpha_i)^j v_i=v_{ij}$ より，

$$(T-\alpha_i)v_{i0} = v_{i1}, \quad (T-\alpha_i)v_{i1} = v_{i2}, \quad \cdots, \quad (T-\alpha_i)v_{i,b_i-1} = v_{ib_i} = 0$$

であるから，

$$\begin{cases} T(v_{i0}) = \alpha_i v_{i0}+v_{i1} \\ T(v_{i1}) = \qquad \alpha_i v_{i1}+v_{i2} \\ \quad\vdots \qquad\qquad\qquad \ddots \\ T(v_{i,b_i-2}) = \qquad\qquad \alpha_i v_{i,b_i-2}+v_{i,b_i-1} \\ T(v_{i,b_i-1}) = \qquad\qquad\qquad \alpha_i v_{i,b_i-1} \end{cases}$$

となり，V の基底 $v_{10}, v_{11}, \cdots, v_{1,b_1-1}, v_{20}, \cdots, v_{2,b_2-1}, \cdots, v_{u0}, \cdots, v_{u,b_u-1}$ に関して T に対応する行列は (3.16) の形となる．その一意性は，(3.15) における $\langle p_i^{b_i}\rangle$ の一意性にほかならない．∎

第4章　直積と正規列

群の構造を記述するもっとも簡単な手段は直積分解や正規列を作ることである．本章ではこれらについての基本事項を説明する．主定理は，組成列に関する Jordan–Hölder の定理と直既約分解に関する Krull-Remak-Schmidt の定理である．大切なことは，これらの結果がいわゆる‘作用域をもつ群’に対しても成り立つことである．このような群を考えることによって定理の含みが多くなり，したがって応用が広くなるという大きな利点がある．最初から‘作用域をもつ群’について述べるのが能率的ではあるが，記述を複雑にしないために，始めは‘作用域をもたない群’の場合を述べ，あとで‘作用域をもつ群’の場合をまとめて述べる．

§4.1　Jordan-Hölder の定理

a)　正規列

群 G の部分群の有限列

$$G = G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1$$

において，G_i が G_{i-1} の正規部分群であるとき，このような列を G の**正規列**（または正規鎖）といい，

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = 1$$

と書く．一般には $G \triangleright G_i$ である必要はないし，また上の部分群の列に重複（すなわち或る i に対し $G_{i-1}=G_i$）があってもかまわない．もちろん重複のあるときには重複項の一つを残し，他を除くことによって重複のない正規列を作ることができる．

G の二つの正規列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = 1, \tag{4.1}$$

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{m-1} \triangleright H_m = 1 \tag{4.2}$$

は，$m=n$ でそれぞれの剰余群の列

$$G_0/G_1, \quad G_1/G_2, \quad \cdots, \quad G_{n-1}/G_n,$$

$$H_0/H_1, \quad H_1/H_2, \quad \cdots, \quad H_{m-1}/H_m$$

が適当な順序で一つずつ同型であるとき，二つの正規列は**同型**であるという．また (4.2) の各項が必ず (4.1) に (重複もこめて) 現われるとき，正規列 (4.1) は正規列 (4.2) の**細分**であるという．

定理 4.1 (Schreier)

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_{n-1} \triangleright H_n = 1,$$
$$G = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_{m-1} \triangleright K_m = 1$$

を G の二つの正規列とする．それぞれを適当に細分して同型な正規列を作ることができる．——

証明はつぎの Zassenhaus の補題を用いる．

補題 4.1 (Zassenhaus)　H, H_1, K, K_1 は G の部分群で $H \triangleright H_1$, $K \triangleright K_1$ とする．このとき，

$$H_1(H \cap K)/H_1(H \cap K_1) \simeq K_1(K \cap H)/K_1(K \cap H_1)$$

である．

証明　$H \triangleright H_1$ だから補題 1.1 により $H_1(H \cap K)$ は H の部分群である．また明らかに

$$H_1(H \cap K) \triangleright H_1, \qquad H \cap K \triangleright H \cap K_1$$

である．$H \cap K$ から $H_1(H \cap K)/H_1$ への自然準同型において，$H \cap K_1$ の像は $H_1(H \cap K_1)/H_1$ であるから $H_1(H \cap K)/H_1 \triangleright H_1(H \cap K_1)/H_1$，したがって $H_1(H \cap K) \triangleright H_1(H \cap K_1)$．またこの準同型による $H_1(H \cap K_1)/H_1$ の逆像は $(H \cap K) \cap H_1(H \cap K_1) = (H_1 \cap K)(H \cap K_1)$．準同型定理，第1同型定理を用いて

$$(4.3) \qquad H \cap K/(H_1 \cap K)(H \cap K_1) \simeq (H_1(H \cap K)/H_1)/(H_1(H \cap K_1)/H_1)$$
$$\simeq H_1(H \cap K)/H_1(H \cap K_1).$$

ところで左辺は H, K に関して対称だから，H と K の役割をかえて

$$(4.4) \qquad H \cap K/(H_1 \cap K)(H \cap K_1) \simeq K_1(K \cap H)/K_1(K \cap H_1)$$

を得る．(4.3)，(4.4) により

$$H_1(H \cap K)/H_1(H \cap K_1) \simeq K_1(K \cap H)/K_1(K \cap H_1)$$

を得る．▌

定理 4.1 の証明　$H_{i-1} \triangleright H_i$, $K_{j-1} \triangleright K_j$ を用いて H_{ij}, K_{ji} をつぎのように定義する：

$$H_{ij}=H_i(H_{i-1}\cap K_j), \qquad K_{ji}=K_j(K_{j-1}\cap H_i).$$

このとき G の長さ mn の二つの正規列でそれぞれもとの正規列の細分であるものができる：

$$G=H_{10}\rhd H_{11}\rhd\cdots\rhd H_{1m}\rhd H_{20}\rhd\cdots,$$
$$G=K_{10}\rhd K_{11}\rhd\cdots\rhd K_{1n}\rhd K_{20}\rhd\cdots.$$

Zassenhaus の補題により $H_{i,j-1}/H_{ij}\simeq K_{j,i-1}/K_{ji}$ であるから，これら二つの正規列は同型である．▌

b）組成列

$$G=G_0\rhd G_1\rhd\cdots\rhd G_{n-1}\rhd G_n=1$$

を重複のない正規列とする．各 i に対し，剰余群 G_{i-1}/G_i が単純群であるとき，すなわち G_{i-1} と G_i の間に G_{i-1}, G_i と異なる G_{i-1} の正規部分群が存在しないとき，このような正規列を**組成列**という．組成列とは重複を許さずにそれ以上細分のできない正規列であるといってもよい．組成列の各剰余群 G_{i-1}/G_i を G の**組成因子**という．一般には，与えられた群が組成列をもつとは限らない．たとえば，無限巡回群 $\boldsymbol{Z}$ は明らかに組成列をもたない．群が組成列をもつための条件については d) で述べるが，組成列をもつ群に対してはつぎの定理がある．

定理 4.2 (Jordan-Hölder の定理) G が少なくとも一つの組成列をもつとする．このとき，重複のない任意の正規列は細分して組成列にすることができる．また，二つの組成列は互いに同型である．

証明 G の組成列 C と正規列 C' が与えられたとする．Schreier の定理によって両者を細分して同型な正規列ができるのであるが，組成列 C の方はそれ以上細分できないのであるから，結局 C' を適当に細分すれば C と同型になる．とくに C, C' がともに組成列ならば，C と C' は始めから同型でなければならない．▌

問 4.1 可解群 G が組成列をもつためには，G が有限群であることが必要十分であることを示せ．

c）主組成列と特組成列

G の正規部分群 G_i の重複のない列

$$G=G_0\supsetneqq G_1\supsetneqq\cdots\supsetneqq G_{n-1}\supsetneqq G_n=1$$

において G_{i-1} と G_i の間に G_{i-1}, G_i と異なる G の正規部分群が存在しないとき，

この列を G の**主組成列**という．G の部分群 H が G の任意の自己同型で不変であるとき，すなわち

$$\sigma(H) = H \qquad (\forall \sigma \in \mathrm{Aut}\,(G))$$

を満たすとき，**特性部分群**とよばれる．特性部分群は正規部分群である．G の特性部分群 G_i の重複のない列

$$G = G_0 \supsetneqq G_1 \supsetneqq \cdots \supsetneqq G_{n-1} \supsetneqq G_n = 1$$

において，G_{i-1} と G_i の間に G_{i-1}, G_i と異なる G の特性部分群が存在しないとき，この列を G の**特組成列**という．ところで主組成列，特組成列に対しても上に述べた Jordan-Hölder の定理が成り立つ．

定理 4.3 G が少なくとも一つ主(特)組成列をもつとする．G の重複のない正規(特性)部分群の任意の列は，細分して主(特)組成列にすることができる．とくに二つの主(特)組成列は同型である．——

証明は定理 4.2 の証明をそのまま真似すればよいのだが，この場合を含めてもっと一般に議論するためには，後に定義する‘作用域をもつ群’の概念が必要になる．これについては §4.3 を参照．

d）極大条件と極小条件

上でも注意したように一般には与えられた群が組成列をもつとは限らない．ここでは組成列をもつための条件について述べる．

極大条件 X を群 G の部分群からなる或る集合とする．X の任意の部分集合が包含関係に関して極大元をもつとき，X は極大条件を満たすという．

X としては通常つぎのものが考えられる：

(i) G のすべての部分群からなる集合，

(ii) G のすべての正規部分群からなる集合，

(iii) G の正規列に現われる部分群——このような部分群を**正規列部分群**(または正規鎖部分群)という——全体の集合．

X が極大条件を満たすとき，X が (i), (ii), (iii) であるのにしたがってそれぞれ G は部分群，正規部分群，正規列部分群について極大条件を満たすという．

双対的に極小条件がまったく同様に定義される．

G が有限群であれば，任意の X は極大条件，極小条件を満たす．また G が Abel 群ならば，上の (i), (ii), (iii) の集合はすべて一致する．

定理 4.4 G が組成列をもつためには，G が正規列部分群について極大条件，極小条件を満たすことが必要十分である．とくに G が部分群について極大条件，極小条件を満たせば，組成列をもつ．

証明 まず条件が十分であることを示そう．つぎの性質をもつ G の真の部分群 H の集合 X を考える：G に始まり H に終る重複のない部分群の列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = H$$

で，G_{i-1}/G_i は単純なるものが存在する．X の元は正規列部分群である．まず X は空集合ではない．なぜなら G の真の正規部分群全体の集合は極大条件により極大元をもつが，それは X に含まれるからである．極小条件により X は極小元 H_0 をもつ．$H_0=1$ を示せばよいから，$H_0 \neq 1$ と仮定して矛盾をだそう．H_0 の真の正規部分群全体の集合 X_0 を考える．X_0 の元は G の正規列部分群であり，$X_0 \ni 1$ だから X_0 は空集合ではない．よって X_0 は極大元 H_1 をもつ．このとき H_0/H_1 は単純だから，$H_1 \in X$．これは H_0 の X での極小性に反する．逆に G は組成列をもつとする．X_0 を G の正規列部分群からなる任意の集合として，X_0 の元の有限列で

$$H_1 \supsetneqq H_2 \supsetneqq \cdots \supsetneqq H_r \qquad (H_i \in X_0) \tag{4.5}$$

なるものを考えると，Jordan-Hölder の定理により G の組成列で(4.5)の各項が現われるものが存在する．したがって(4.5)のような列で長さ最大のものが存在し，そのとき H_1 が X_0 の極大元，H_r が X_0 の極小元である．∎

問 4.2 つぎのことを示せ．(i) 加法群 $\boldsymbol{Z}$ は部分群について極大条件を満たすが極小条件を満たさない．(ii) p を素数とする．$G(p)=\{\omega \in \boldsymbol{C}^* \mid \omega^{p^n}=1,\ 0<n \in \boldsymbol{Z}\}$ は部分群について極小条件を満たすが極大条件を満たさない．(iii) 有理数の加法群 $\boldsymbol{Q}$ は極大条件も極小条件も満たさない．

問 4.3 群 G が主組成列をもつためには，G が正規部分群について極大条件，極小条件を満たすことが必要十分である．

問 4.4 $G \rhd N$ とする．G が部分群について極大条件を満たすためには，G/N，N が部分群について極大条件を満たすことが必要十分である．極小条件についても同様である．また正規列部分群に対しても同じことが成り立つ．正規部分群に対してはどうか．――

極大条件のつぎの性質は大切である．

定理 4.5　つぎの条件は同値である:

(i)　G は部分群について極大条件を満たす,

(ii)　G の各部分群は有限生成である. ——

この定理の証明には, いわゆる Zorn の補題が用いられる. ここで Zorn の補題を簡単に説明しておこう.

集合 X につぎの三つの条件を満たす関係 $\leqq$ が定義されているとき, この関係 $\leqq$ を X の**順序**といい, X は(この関係に関して)**順序集合**であるといわれる:

(i)　$x \leqq x \quad (\forall x \in X)$,

(ii)　$x \leqq y,\ y \leqq x \Longrightarrow x = y$,

(iii)　$x \leqq y,\ y \leqq z \Longrightarrow x \leqq z$.

たとえば, S を任意の集合, S の部分集合全体の集合を X とする. $X \ni x, y$ に対して包含関係 $x \subseteq y$ は, 上の条件(i), (ii), (iii)を満たすから X の順序となる.

上の(i), (ii), (iii)に加えて

(iv)　X の任意の2元 x, y に対して $x \leqq y$ または $y \leqq x$

が成り立つとき, X を**全順序集合**という. 順序集合 X の部分集合 Y に対して $x \geqq y\ (\forall y \in Y)$ なる x を Y の**上界**という. また $X \ni x$ が

$$x \leqq y \quad (y \in X) \Longrightarrow x = y$$

なる条件を満たすとき, このような x を X の**極大元**という. さて Zorn の補題といわれるのはつぎの命題である.

Zorn の補題　X を順序集合とする. X の部分集合が(X における順序に関して)全順序集合であるときつねに上界をもてば, X は極大元をもつ. ——

この補題の証明については, 集合論の書物を参照されたい. 少なくとも本講では, これは公理だと思って差し支えはない.

さて Zorn の補題を用いて定理 4.5 を証明しよう.

定理 4.5 の証明　(i) $\Longrightarrow$ (ii): H を G の部分群とする. H の有限生成部分群全体の集合を X とする. 仮定(i)により X は極大元 H_0 をもつ. $H \neq H_0$ とすると, $H - H_0 \ni x$ をとれば, $\langle H_0, x\rangle = K$ は H の有限生成部分群だから $K \in X$. $H_0 \subsetneqq K$ だから, これは H_0 の極大性に反する. したがって $H = H_0$, すなわち H は有限生成である.

(ii) $\Longrightarrow$ (i): ここで Zorn の補題を用いる. X を G の部分群からなる任意の

集合とする．X を包含関係に関して順序集合と見る．$\{H_\lambda \mid \lambda \in \Lambda\}$ を X の全順序部分集合とするとき，$H=\bigcup_\lambda H_\lambda$ は G の部分群である．仮定(ii)により H は有限生成だから $H=\langle h_1, h_2, \cdots, h_n\rangle$ とすると，$h_i \in H_{\lambda_i}$ なる $\lambda_i \in \Lambda$ が存在する．$\{H_\lambda\}$ は全順序集合だから，$H_{\lambda_{i_0}} \supseteq H_{\lambda_j}$ $(j=1, 2, \cdots, n)$ なる i_0 が存在する．このとき，$h_i \in H_{\lambda_{i_0}}$，よって $H \subseteq H_{\lambda_{i_0}} \subseteq H$，したがって $H=H_{\lambda_{i_0}} \in X$ を得る．これは $\{H_\lambda \mid \lambda \in \Lambda\}$ が X で上界をもつことを示すから Zorn の補題が適用できて，X が極大元をもつことがわかる．▌

§4.2 Krull-Remak-Schmidt の定理

a) 直積分解

G を $G_1, G_2, \cdots, G_n$ の直積としよう：$G=G_1 \otimes G_2 \otimes \cdots \otimes G_n$.

$$G_i' = \{(e_1, \cdots, e_{i-1}, x_i, e_{i+1}, \cdots, e_n) \in G \mid x_i \in G_i\} \qquad (e_i \text{ は } G_i \text{ の単位元})$$

とおくと，明らかに $(e_1, \cdots, x_i, \cdots, e_n) \mapsto x_i$ なる対応によって

$$G_i' \simeq G_i$$

である．以後この同型で G_i' と G_i を同一視して G_i を G の部分群と考えよう．このとき，つぎが成り立つことが容易にわかる：

(α) $G \triangleright G_i$,

(β) $G = G_1 G_2 \cdots G_n$,

(γ) G の各元 x は $x=x_1 x_2 \cdots x_n$ $(x_i \in G_i)$ なる形に一意的に書ける．

問 4.5 上の(α), (β), (γ)を確かめよ．——

逆に G の部分群 G_i が上の条件(α), (β), (γ)を満たすとする．このとき，

(δ) $G_i \cap G_j = 1 \quad (i \neq j)$,

(ε) $G_i \ni x_i,\ G_j \ni x_j \ (i \neq j) \Longrightarrow x_i x_j = x_j x_i$

が成り立つ．実際，$x \in G_i \cap G_j$ ならば，$x_i=x$，$x_k=1$ $(k \neq i)$，$y_j=x$，$y_l=1$ $(l \neq j)$ とすると $x=x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$ であるから，(γ)により $x_i=y_i=1$，よって $x=1$ となり(δ)が成り立つ．また $G_i \ni x_i$，$G_j \ni x_j$ とすると，$G \triangleright G_j$ より $x_i^{-1} x_j^{-1} x_i \in G_j$，よって $x_i^{-1} x_j^{-1} x_i x_j = (x_i^{-1} x_j^{-1} x_i) x_j \in G_j$．同様に $x_i^{-1} x_j^{-1} x_i x_j = x_i^{-1}(x_j^{-1} x_i x_j) \in G_i$．したがって(δ)により，$x_i^{-1} x_j^{-1} x_i x_j \in G_i \cap G_j = 1$，すなわち $x_i x_j = x_j x_i$ となり，(ε)が成り立つ．

(ε)を用いて G から $G_1 \otimes G_2 \otimes \cdots \otimes G_n$ への写像

$$G \ni x = x_1x_2\cdots x_n \longmapsto (x_1, x_2, \cdots, x_n) \in G_1 \otimes G_2 \otimes \cdots \otimes G_n$$

は，G から $G_1 \otimes \cdots \otimes G_n$ の上への同型であることがわかる．以上により G が

$$G \simeq G_1 \otimes G_2 \otimes \cdots \otimes G_n$$

なる直積分解をもつためには，G が (α), (β), (γ) を満たす部分群 $G_1, G_2, \cdots, G_n$ をもつことが必要十分であることがわかった．したがって以後 $G_1, G_2, \cdots, G_n$ が (α), (β), (γ) を満たす G の部分群のとき，

$$G = G_1 \otimes G_2 \otimes \cdots \otimes G_n$$

と書くことにしよう．

問 4.6　$G = G_1G_2\cdots G_n \triangleright G_i$ $(i=1, 2, \cdots, n)$ とする．つぎの条件は同値である：

(i)　$G = G_1 \otimes G_2 \otimes \cdots \otimes G_n$,

(ii)　$x_1x_2\cdots x_n = 1 \quad (x_i \in G_i) \Longrightarrow x_i = 1 \quad (\forall i)$,

(iii)　$G_i \cap (G_{i+1}\cdots G_n) = 1 \quad (i=1, 2, \cdots, n-1)$. ——

群 G はつねに $G = G \otimes 1$ なる直積分解をもつ．このような直積分解を**自明な直積分解**という．G の直積分解が自明なものに限るとき，G は**直既約**であるという．また

$$G = G_1 \otimes G_2 \otimes \cdots \otimes G_n$$

のとき各 i に対して $G_i \neq 1$ で G_i が直既約ならば，このような直積分解を G の**直既約分解**という．

問 4.7　$\boldsymbol{Z}$, $G(p)$, $\boldsymbol{Q}$ は直既約である．($G(p)$ の定義は問 4.2 を参照.) また有限巡回群が直既約であるためには，位数が素数べキであることが必要十分である．——

一般には与えられた群が直既約分解をもつとは限らないが，直既約分解をもつための簡単な十分条件としてつぎの補題がある．

補題 4.2　G が正規部分群について極大条件を満たせば，G は直既約分解をもつ．

証明　G は直既約でないとしてよい．G の自明でない直積因子全体の集合を X とする：

$$X = \{G_1 \subsetneqq G \mid 1 \neq \exists G_2 \subsetneqq G,\ G = G_1 \otimes G_2\}.$$

G は直既約でないから，X は空集合ではない．仮定により X は極大元 G_0 をもつ．このとき $G = G_0 \otimes H$ なる $H \neq 1$ が存在するが，G_0 の極大性により H は直

既約でなければならない．つぎに G の自明でない直積因子で直既約分解をもつもの全体の集合 X_0 を考える：

$$X_0=\{G_0 \subsetneqq G \mid \exists N \subsetneqq G,\ G=G_0 \otimes N,\ G_0=G_1 \otimes \cdots \otimes G_r,\ G_i \text{ は直既約}\}.$$

上述により X_0 は空集合ではない．X_0 の極大元 G_0 をとれば，$G=G_0\otimes N$ とするとき，N は直既約でなければならない．実際 N が直既約でないとして N の自明でない直積因子の集合を X_1 とすると，X_1 は極大元 N_1 をもち $N=N_1\otimes N_2$ なる N_2 が存在する．しかも N_1 の極大性により N_2 は直既約である．このとき，$G_0\otimes N_2 \in X_0$ となり，G_0 の極大性に反する．したがって G も直既約分解をもつ．▌

G が二つの直既約分解

$$G=G_1\otimes G_2\otimes\cdots\otimes G_m=H_1\otimes H_2\otimes\cdots\otimes H_n$$

をもったとしよう．このときこれら二つの直既約分解の間の関係はどうであろうか．この問に答えるのが，後に述べる Krull-Remak-Schmidt の定理である．

b）自己準同型

直積分解を調べるために群の自己準同型が大切な役割を果たす．群 G の自己準同型（G から G への準同型）全体の集合を $\mathrm{End}(G)$ で表わそう．$\mathrm{End}(G)$ は写像の積に関して半群である．ただし以後 $x\in G$, $\sigma\in\mathrm{End}(G)$ に対して x の σ による像を x^σ で表わし，写像の積は

$$x^{\sigma\tau}=(x^\sigma)^\tau \qquad (\sigma,\tau\in\mathrm{End}(G))$$

によって定義することにする．G の各元 x に単位元 1 を対応させる写像は G の自己準同型である．これを 0 で表わす：

$$x^0=1 \qquad (\forall x\in G).$$

また G の恒等写像は，半群 $\mathrm{End}(G)$ の単位元であるが，これは 1 で表わされる：

$$x^1=x \qquad (\forall x\in G).$$

これを G の単位元と混同しないように注意すべきである．$\mathrm{End}(G)\ni\sigma,\tau$ は

$$x^\sigma x^\tau=x^\tau x^\sigma \qquad (\forall x\in G)$$

なる条件を満たすとき，**加法可能**といわれる．このとき写像

$$x\longmapsto x^\sigma x^\tau$$

は G の自己準同型である．これを $\sigma+\tau$ で表わす：

$$x^{\sigma+\tau}=x^\sigma x^\tau.$$

つぎのことは容易に確かめられる：

(4.6)　$\mathrm{End}(G) \ni \sigma, \tau, \rho$ のどの二つも加法可能ならば

$$(\sigma+\tau)+\rho = \sigma+(\tau+\rho),$$

(4.7)　$\mathrm{End}(G) \ni \sigma, \tau, \rho$ で，σ と τ が加法可能ならば

$$\sigma+\tau = \tau+\sigma,$$
$$\rho(\sigma+\tau) = \rho\sigma+\rho\tau,$$
$$(\sigma+\tau)\rho = \sigma\rho+\tau\rho.$$

問 4.8　(4.6), (4.7)を確かめよ．とくに G が Abel 群ならば $\mathrm{End}(G)$ は環となる．——

$\mathrm{End}(G) \ni \sigma$ が G のすべての内部自己同型と可換であるとき，すなわち

(4.8)
$$(y^{-1}xy)^{\sigma} = y^{-1}x^{\sigma}y \qquad (\forall x, y \in G)$$

が成り立つとき，σ を**正規**自己準同型という．$\mathrm{End}(G) \ni 0, 1$ は正規である．また $G=G_1\otimes G_2\otimes\cdots\otimes G_n$ のとき，$G \ni x=x_1x_2\cdots x_n$ に x_i を対応させる写像 ε_i は G の正規自己準同型である．このような写像 ε_i を G から G_i への**射影**という．このとき，$\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ のどの二つも加法可能で

$$1 = \varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n, \qquad \varepsilon_i\varepsilon_j = \varepsilon_j\varepsilon_i = 0 \quad (i \neq j)$$

が成り立つ．

問 4.9　G の正規自己準同型の像は G の正規部分群である．また自己同型 σ が正規であるためには $y^{-1}y^{\sigma} \in Z(G)$ $(\forall y \in G)$ であることが必要十分である．このとき $y^{-1}y^{\sigma}=c(y,\sigma)$ とおくと，$c(y_1y_2,\sigma)=c(y_1,\sigma)c(y_2,\sigma)$ $(y_i \in G)$ であることを示せ．——

つぎの補題は基本的である．

補題 4.3 (Fitting)　G は正規部分群について極大条件，極小条件を満たすとする．$\mathrm{End}(G) \ni \sigma$ が正規のとき，或る自然数 N が存在して $N \leqq k$ なる任意の k に対して

$$G = G^{\sigma^k}\otimes G_{\sigma^k}.$$

ここで G^{σ^k} は σ^k の像，G_{σ^k} は σ^k の核を表わす．

証明　$G \supseteqq G^{\sigma} \supseteqq G^{\sigma^2} \supseteqq \cdots$ であるから，極小条件により或る k が存在して

(4.9)
$$G^{\sigma^k} = G^{\sigma^{k+1}} = \cdots$$

である．また $1 \subseteqq G_{\sigma} \subseteqq G_{\sigma^2} \subseteqq \cdots$ であるから極大条件により或る l が存在して

(4.10) $$G_{\sigma^l} = G_{\sigma^{l+1}} = \cdots$$

である．つぎを示そう：

(4.9)′ 或る k に対し $G^{\sigma^k} = G^{\sigma^{k+1}} \Longrightarrow G = G_{\sigma^n} G^{\sigma^n}$ $(n \geqq k)$,

(4.10)′ 或る l に対し $G_{\sigma^l} = G_{\sigma^{l+1}} \Longrightarrow G_{\sigma^n} \cap G^{\sigma^n} = 1$ $(n \geqq l)$.

$G^{\sigma^k}=G^{\sigma^{k+1}}$ ならば，$G^{\sigma^k}=G^{\sigma^{k+1}}=G^{\sigma^{k+2}}=\cdots$ である．$G \ni x$ に対して，$x^{\sigma^k} \in G^{\sigma^k}=G^{\sigma^{2k}}$，よって或る $y \in G$ が存在して $x^{\sigma^k}=y^{\sigma^{2k}}$．このとき，$x^{-1}y^{\sigma^k} \in G_{\sigma^k}$，$y^{\sigma^k} \in G^{\sigma^k}$．したがって $x=(x^{-1}y^{\sigma^k})^{-1}y^{\sigma^k} \in G_{\sigma^k}G^{\sigma^k}$．$n \geqq k$ のとき，$G_{\sigma^k} \subseteqq G_{\sigma^n}$，$G^{\sigma^k}=G^{\sigma^n}$ だから (4.9)′ が得られた．つぎに $G_{\sigma^l} \cap G^{\sigma^l} \ni x$ とすると，$x=y^{\sigma^l}$ $(y \in G)$，よって $1=x^{\sigma^l}=y^{\sigma^{2l}}$，したがって $y \in G_{\sigma^{2l}}$，$G_{\sigma^l}=G_{\sigma^{2l}}$ より $y \in G_{\sigma^l}$．すなわち $x=1$．これは (4.10)′ を示す．

さて (4.9), (4.10) のように k, l をとり，$n \geqq \max(k, l)$ とすると，(4.9)′, (4.10)′ により

$$G = G_{\sigma^n} G^{\sigma^n}, \qquad G_{\sigma^n} \cap G^{\sigma^n} = 1.$$

したがって $G=G_{\sigma^n} \otimes G^{\sigma^n}$ である．▌

系 補題 4.3 の G, σ に対して，つぎの (i), (ii), (iii) が成り立つ．

(i) σ は全射 $\Longleftrightarrow$ σ は単射．

(ii) G が直既約ならば，σ は自己同型であるかあるいはベキ零，すなわち或る n に対して $\sigma^n=0$ である．とくに $G^\sigma=G^{\sigma^2} \neq 1$ ならば σ は自己同型である．

(iii) G は直既約で，σ, τ が加法可能な正規自己準同型で，$\sigma+\tau$ が自己同型ならば，σ, τ の少なくとも一方は自己同型である．

証明 (i) $G=G^\sigma$ とすると $G=G^{\sigma^k}$ $(k=1, 2, \cdots)$．Fitting の補題により十分大きい n に対して $G_{\sigma^n}=1$．したがって $G_\sigma \subseteqq G_{\sigma^n}=1$．すなわち σ は単射である．逆に $G_\sigma=1$ ならば，$G_{\sigma^k}=1$ $(k=1, 2, \cdots)$．再び Fitting の補題により十分大きな n に対して $G=G^{\sigma^n}$，よって $G=G^\sigma$ である．(ii) G は直既約だから十分大きな n に対し $G^{\sigma^n}=1$ または $G_{\sigma^n}=1$．$G^{\sigma^n}=1$ ならば，σ はベキ零である．$G_{\sigma^n}=1$ ならば $G_\sigma=1$，(i) により σ は全射でもあるから，σ は自己同型である．(iii) $\rho=\sigma+\tau$ が自己同型とする．$1=(\sigma+\tau)\rho^{-1}=\sigma\rho^{-1}+\tau\rho^{-1}$ において，$\sigma'=\sigma\rho^{-1}$，$\tau'=\tau\rho^{-1}$ とおくと $\sigma'\tau'=\tau'\sigma'$ である．実際，$1=\sigma'+\tau'$ より $\tau'=\tau'\sigma'+\tau'^2=\sigma'\tau'+\tau'^2$ だから，$\forall x \in G$ に対して $x^{\tau'}=x^{\tau'\sigma'}x^{\tau'^2}=x^{\sigma'\tau'}x^{\tau'^2}$ となり $x^{\tau'\sigma'}=x^{\sigma'\tau'}$ を得る．σ', τ' がともにベキ零ならば，2 項定理により $\sigma'+\tau'$ もベキ零．しかるに $\sigma'+\tau'=1$ であるか

ら，$\sigma'+\tau'$ はベキ零にはなり得ない．よって σ', τ' の少なくとも一方はベキ零ではない．それを σ' とすると，(ii) により σ' は自己同型，したがって $\sigma=\sigma'\rho$ も自己同型である．▌

c) Krull-Remak-Schmidt の定理

定理 4.6 (Krull-Remak-Schmidt の定理)[1]　G は正規部分群について極大条件，極小条件を満たすとする．このとき，

(i) G は少なくとも一つの直既約分解をもつ．

(ii) $G=H_1\otimes H_2\otimes\cdots\otimes H_m=K_1\otimes K_2\otimes\cdots\otimes K_n$ を G の直既約分解とする．このとき，任意の $H_1, H_2, \cdots, H_r$ $(1\leqq r\leqq m)$ に対して，$K_{j_1}, K_{j_2}, \cdots, K_{j_r}$ を適当にとれば，G の正規自己同型 σ が存在して

$$G = K_{j_1}\otimes K_{j_2}\otimes\cdots\otimes K_{j_r}\otimes H_{r+1}\otimes\cdots\otimes H_m,$$
$$H_i^\sigma = K_{j_i} \qquad (1\leqq i\leqq r),$$
$$\sigma \text{ は } H_{r+1}\otimes\cdots\otimes H_m \text{ の上では恒等写像}$$

となる．とくに $m=n$ かつ $H_1, H_2, \cdots, H_m$ と $K_1, K_2, \cdots, K_m$ は適当な順序で一つずつ同型である．

証明　補題 4.2 により (i) が成り立つ．(ii) を示すために最初につぎのことを証明しよう：

(4.11)　$G=H\otimes G_1=K_1\otimes K_2\otimes\cdots\otimes K_n$，$H, K_1, K_2, \cdots, K_n$ は直既約とするとき G の正規自己同型 σ と或る K_i が存在して，$H^\sigma=K_i$ かつ σ は G_1 の各元を自分自身にうつす．

$\varepsilon, \delta, \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ をそれぞれ G から $H, G_1, K_1, K_2, \cdots, K_n$ への射影とする．$\varepsilon, \delta, \varepsilon_i$ $(1\leqq i\leqq n)$ は G の正規自己準同型で

$$1 = \varepsilon+\delta = \varepsilon_1+\varepsilon_2+\cdots+\varepsilon_n$$

である．$\varepsilon=\varepsilon_1\varepsilon+\varepsilon_2\varepsilon+\cdots+\varepsilon_n\varepsilon$ は H の恒等写像であるから，Fitting の補題の系の (iii) により，$\varepsilon_1\varepsilon, \varepsilon_2\varepsilon, \cdots, \varepsilon_n\varepsilon$ の少なくとも一つは H の自己同型である．それを $\varepsilon_i\varepsilon$ とする．このとき，明らかに $H=H^{\varepsilon_i\varepsilon}\subseteqq K_i^\varepsilon\subseteqq H$ であるから

(4.12)　$$H = K_i^\varepsilon = H^{\varepsilon_i\varepsilon}$$

---

1) この定理を 'Remak-Schmidt の定理' といい，後に述べる作用域をもつ群についての対応する定理を 'Krull-Remak-Schmidt の定理' というのがより正確である．しかし本質的内容はまったく同じなので本書ではこのようにいうことにする．

を得る．つぎに

(4.13) $$H^{\varepsilon_i}=K_i$$

を示そう．実際，

$$\begin{aligned} K_i^{(\varepsilon\varepsilon_i)^2} &= K_i^{\varepsilon\varepsilon_i\varepsilon\varepsilon_i} \\ &= H^{\varepsilon_i\varepsilon\varepsilon_i} && \text{((4.12) の最初の等号)} \\ &= K_i^{\varepsilon\varepsilon_i} && \text{((4.12) の第 2 の等号の両辺を } \varepsilon_i \text{ 乗)} \\ &= H^{\varepsilon_i} \neq 1 && (H^{\varepsilon_i}=1 \text{ なら (4.12) により } H=1 \text{ となる}) \end{aligned}$$

であるから，Fitting の補題の系の (ii) により $\varepsilon\varepsilon_i$ は K_i の自己同型となり，$K_i=K_i^{\varepsilon\varepsilon_i}=H^{\varepsilon_i}$. すなわち (4.13) を得る．$\varepsilon\varepsilon_i$ と $\delta\varepsilon_j\,(j=1,2,\cdots,n)$ は加法可能だから，$\varepsilon\varepsilon_i$ と $\delta=\delta\varepsilon_1+\cdots+\delta\varepsilon_n$ は加法可能である．$\sigma=\varepsilon\varepsilon_i+\delta$ とおく．この σ と K_i が (4.11) で求めているものであることを示そう．明らかに σ は正規自己準同型である．σ が単射であることをみるために，$x^\sigma=1\ (x\in G)$ とする．このとき

$$1=x^{\sigma\varepsilon}=x^{\varepsilon\varepsilon_i\varepsilon+\delta\varepsilon}=x^{\varepsilon\varepsilon_i\varepsilon}$$

であって，$x^\varepsilon\in H$ かつ $\varepsilon_i\varepsilon$ は H の自己同型だから，$x^\varepsilon=1$ を得る．したがって $1=x^\sigma=x^{\varepsilon\varepsilon_i+\delta}=x^\delta$. よって

$$x=x^\varepsilon x^\delta=1$$

となる．Fitting の補題の系の (i) により，σ は全射でもあるから σ は G の自己同型となる．また

$$\begin{aligned} H^\sigma &= H^{\varepsilon\varepsilon_i+\delta}=H^{\varepsilon_i}=K_i && \text{(最後の等号は (4.13) による)}, \\ x^\sigma &= x^{\varepsilon\varepsilon_i+\delta}=x^\delta=x && (\forall x\in G_1) \end{aligned}$$

であるから，σ と K_i は (4.11) のすべての条件を満たすことがわかった．

定理の主張 (ii) を r に関する帰納法によって示そう．$r=1$ のときは，$H_1=H$, $H_2\otimes H_3\otimes\cdots\otimes H_m=G_1$ として (4.11) を適用すればよい．$H_1,H_2,\cdots,H_{r-1}$ に対して G の正規自己同型 σ_{r-1} と $K_{j_1},K_{j_2},\cdots,K_{j_{r-1}}$ が存在して

(4.14)
$$\begin{aligned} &G=K_{j_1}\otimes K_{j_2}\otimes\cdots\otimes K_{j_{r-1}}\otimes H_r\otimes H_{r+1}\otimes\cdots\otimes H_m, \\ &H_i^{\sigma_{r-1}}=K_{j_i} \qquad (1\leqq i\leqq r-1), \\ &\sigma_{r-1} \text{ は } H_r\otimes\cdots\otimes H_m \text{ の上で恒等写像} \end{aligned}$$

であると仮定する．このとき (4.14) において，$H_r=H$, $K_{j_1}\otimes\cdots\otimes K_{j_{r-1}}\otimes H_{r+1}\otimes\cdots\otimes H_n=G_1$ として (4.11) を適用すれば，G の正規自己同型 σ と K_{j_r} が存在して

$$G = K_{j_1}\otimes\cdots\otimes K_{j_r}\otimes H_{r+1}\otimes\cdots\otimes H_m,$$
$$H_r{}^\sigma = K_{j_r},$$
$$\sigma \text{ は } H_{r+1}\otimes\cdots\otimes H_m \text{ の上で恒等写像}$$

となる．このとき $\sigma_r=\sigma_{r-1}\sigma$ と $K_{j_1}, K_{j_2}, \cdots, K_{j_r}$ が定理の主張(ii)で求めているものになることが容易にわかる．▌

一般には，G の直既約分解

$$G = G_1\otimes G_2\otimes\cdots\otimes G_n$$

において，$G_1, G_2, \cdots, G_n$ は一意的には定まらないが，正規部分群についての極大，極小条件のもとで，G が完全群あるいは G の中心が単位群であれば，$G_1, G_2, \cdots, G_n$ は G に対して一意的に定まる．

問 4.10 このことを確かめよ．[ヒント] 問 4.9 を参照．——

最後に単純群の直積について注意しておこう．つぎの補題は§5.3で用いられるであろう．

補題 4.4 (i) G が非可換単純群 $G_1, G_2, \cdots, G_n$ の直積ならば直積因子 $G_1, G_2, \cdots, G_n$ は G に対して一意的に定まる．また G の正規部分群は $G_1, G_2, \cdots, G_n$ のいくつかの直積である．(ii) G の正規部分群 N_1, N_2 がそれぞれ非可換単純群の直積ならば，その積もそうである．(iii) G を組成列をもつ群とするとき，G の極小正規部分群は基本 Abel 群であるかあるいは同型な非可換単純群いくつかの直積である．

証明 (i) の前半は上の問 4.10 からわかる．N を G の正規部分群とするとき，G_1 の単純性から $N\supseteqq G_1$ または $N\cap G_1=1$，よって $NG_1=N$ または $N\otimes G_1$．G_2 の単純性から，$NG_1\supseteqq G_2$ または $NG_1\cap G_2=1$．よって $NG_1G_2=NG_1$，$NG_1G_2=N\otimes G_2$ または $NG_1G_2=N\otimes G_1\otimes G_2$．これを続けて

$$G = NG_1G_2\cdots G_n = N\otimes G_{i_1}\otimes\cdots\otimes G_{i_r} \qquad (1\leqq i_1<\cdots<i_r\leqq n)$$

を得る．直積因子 $G_1, G_2, \cdots, G_n$ の一意性により，N の直積分解を考えて N はそれらのいくつかの直積でなければならない．(ii) (i) を用いれば，$N_i=(N_1\cap N_2)\otimes M_i$ $(i=1,2)$，$M_i\lhd G$ が容易にわかるから $N_1N_2=(N_1\cap N_2)\otimes M_1\otimes M_2$ となる．(iii) G の極小正規部分群を N, N の極小正規部分群を N_1 としよう．まず N の極小性から $N=\langle N_1{}^x \mid x\in G\rangle$ である．$N_1{}^x$ $(x\in G)$ 達の有限個の積全体の集合を考え，その極大元を N_0 とすると $N_0\supseteqq N^x$ $(\forall x\in G)$ だから $N=N_0$．このと

き N_1 の極小性から N は有限個の $N_1{}^x$ の直積であることは見易い．よって $N=N_1{}^{x_1}\otimes N_1{}^{x_2}\otimes\cdots\otimes N_1{}^{x_r}$ とするとき，$N_1{}^{x_i}$ の正規部分群は N の正規部分群だから N_1 の極小性より $N_1{}^{x_i}(1\leqq i\leqq r)$ は単純群，したがってそれは素数位数の群であるか非可換単純群である．▌

§4.3 作用域をもつ群

§4.1-§4.2 で群の正規列と直積分解に関する基本事項について述べた．本節では‘作用域をもつ群’の概念を導き，これらの群に対しても §4.1-§4.2 の結果が成り立つことを注意する．またこのような一般化がいかに有効であるかを示す簡単な応用例について説明する．

Σ を集合，G を群とする．$G\times\Sigma$ から G への写像

$$G\times\Sigma\ni(x,\sigma)\longmapsto x^\sigma\in G$$

が定義されていて

$$(xy)^\sigma=x^\sigma y^\sigma \qquad (\forall x,y\in G)$$

が成り立つとき，Σ は G に**作用する**という．また Σ を**作用域**，G を Σ **群**という．簡単に (G,Σ) を Σ 群ということもある．Σ の各元が G の恒等写像をひき起しているとき，Σ 群は単なる群の概念に他ならない．この意味で Σ 群の概念は，群の概念の拡張である．なお，応用上は Σ が半群あるいは環であることが多いが，一般には Σ に何の代数的構造も考えない．

以下，(G,Σ) を Σ 群とする．

(α) G の部分集合 S と $\Sigma\ni\sigma$ に対して

$$S^\sigma=\{s^\sigma\mid s\in S\}$$

とおく．$S^\sigma\subseteqq S\ (\forall\sigma\in\Sigma)$ のとき，S は Σ **不変**であるという．Σ 不変な部分群，正規部分群をそれぞれ Σ 部分群，Σ 正規部分群という．或る有限集合 S に対して

$$G=\langle S,S^\sigma\mid\sigma\in\Sigma\rangle$$

のとき，Σ 群 G は有限生成であるという．

(β) N を G の Σ 正規部分群とする．剰余群 $\bar{G}=G/N$ を自然に Σ 群とみることができる：$\bar{G}\ni\bar{x}$，$\Sigma\ni\sigma$ に対して

$$\bar{x}^\sigma=\overline{x^\sigma}$$

とおくと，Σ が $\bar{G}$ に作用していることが容易にわかる．$(\bar{G}, \Sigma)$ を (G, Σ) の剰余群という．

(γ) Σ 群 G の Σ 正規部分群が自明なもの（すなわち G 自身と単位群）に限るとき，G を Σ **単純**あるいは Σ **既約**という．

(δ) $(G_1, \Sigma), (G_2, \Sigma)$ を Σ 群とする．G_1 から G_2 への準同型 f が

$$f(x^\sigma) = f(x)^\sigma \qquad (\forall x \in G_1,\ \forall \sigma \in \Sigma)$$

なる条件を満たすとき，f を Σ **準同型**という．とくにこのような f が G_1 から G_2 の上への全単射のとき，f を G_1 から G_2 の上への Σ **同型**という．Σ 準同型の像や核は，Σ 不変である．——

さて§4.1-§4.2で定義した正規列，組成列，極大条件，極小条件，直積分解，直既約分解の概念は，それらの定義に現われる部分群を Σ 部分群だけに限定することにより Σ 群に対しても定義される．たとえば，Σ 群 G の Σ 部分群の有限列

$$G = G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1$$

において，$G_{i-1} \triangleright G_i$ $(i=1, 2, \cdots, n)$ であれば，この列は Σ **正規列**，さらに各 i に対し $G_{i-1} \neq G_i$ で G_{i-1}/G_i が Σ 単純ならば，この列は Σ **組成列**といわれる．また，§1.3で述べた準同型定理，第1，第2同型定理を初めとして，§4.1-§4.2で述べたすべての定理や補題はそれらの証明とともに，そこに現われる部分群や準同型を Σ 部分群，Σ 準同型に限定することによりそのままの形で成り立つ．復習をかねて読者自ら確かめられたい．念のため基本的な定理を Σ 群に対して再録しておこう．

定理 4.2′ (Jordan-Hölder) Σ 群 G が少なくとも一つの Σ 組成列をもつとする．G の重複のない任意の Σ 正規列は細分して Σ 組成列にすることができる．とくに二つの Σ 組成列は必ず同型である．

定理 4.4′ Σ 群 G が Σ 組成列をもつためには，Σ 正規列に現われる Σ 部分群全体の集合が，極大条件，極小条件を満たすことが必要十分である．とくに Σ 群が Σ 部分群について極大条件，極小条件を満たせば，Σ 組成列をもつ．

定理 4.5′ Σ 群に対してつぎの条件は同値である：

(i) Σ 部分群について極大条件を満たす，

(ii) G の任意の Σ 部分群は有限生成である．

定理 4.6′ (Krull-Remak-Schmidt)　Σ 群 G が Σ 正規部分群について極大条件，極小条件を満たすとする．このとき，

（i）G は直既約分解をもつ．

(ii) $G=H_1\otimes H_2\otimes\cdots\otimes H_m=K_1\otimes K_2\otimes\cdots\otimes K_n$ を Σ 群 G の直既約分解とする．任意の $H_1, H_2, \cdots, H_r$ $(1\leqq r\leqq m)$ に対して G の正規 Σ 自己同型 σ と $K_{j_1}, K_{j_2}, \cdots, K_{j_r}$ が存在して

$$G = K_{j_1}\otimes K_{j_2}\otimes\cdots\otimes K_{j_r}\otimes H_{r+1}\otimes\cdots\otimes H_m,$$
$$H_i^{\sigma} = K_{j_i} \qquad (1\leqq i\leqq r),$$
$$\sigma \text{ は } H_{r+1}\otimes\cdots\otimes H_m \text{ の上で恒等写像}$$

となる．とくに $m=n$ で $H_1, H_2, \cdots, H_m$ と $K_1, K_2, \cdots, K_m$ は適当な順序で一つずつ同型である．——

例 4.1　G を任意の群とする．Σ として G の内部自己同型群 $\mathrm{Inn}(G)$ をとると，G は自然に Σ 群と見れる．このときの Σ 組成列が §4.1, c) で定義した主組成列である．また Σ として G の全自己同型群 $\mathrm{Aut}(G)$ をとれば，このときの Σ 組成列が，特組成列に他ならない．また主組成列，特組成列に対する定理 4.3 は，上の定理 4.2′ の特別の場合である．

例 4.2　斜体上の線型空間　V を斜体 Σ 上の線型空間とする．$\Sigma\ni\alpha$, $V\ni v$ に対して

$$v^{\alpha} = \alpha v \qquad (\text{右辺は線型空間におけるスカラー積})$$

とおけば，線型空間の公理 III により

$$(v_1+v_2)^{\alpha} = \alpha(v_1+v_2) = \alpha v_1+\alpha v_2 = v_1^{\alpha}+v_2^{\alpha}$$

であるから，V は Σ 群となる．このとき Σ 部分群は V の部分空間に他ならない．また1次元部分空間は，Σ 単純な Σ 部分群である．よって V は Σ 部分群について極小条件を満たしている．したがって V が部分空間について極大条件を満たすことと，V が Σ 組成列をもつこととは同値である（定理 4.4′）．さらに V が Σ 組成列をもつことは，明らかに V が有限次元であることと同値である．Jordan-Hölder の定理から，とくに有限次元線型空間の次元の一意性がわかる．§1.7 では，このことを別の方法で示したのであった．

例 4.3　$\mathfrak{R}$ を環，V を左 $\mathfrak{R}$ 加群とする．（以下に述べることは‘左’を‘右’におきかえれば，右 $\mathfrak{R}$ 加群に対しても成り立つ.）V は $\mathfrak{R}$ を作用域 Σ とする加群と

考えることができる．この場合の Σ 部分群は $\mathfrak{R}$ 部分加群であり，とくに $V=\mathfrak{R}$ であればそれは $\mathfrak{R}$ の左イデアルのことである．応用上つぎの補題は大切である．

補題 4.5　$\mathfrak{R}$ は左イデアルについて極大条件を満たすとする．このとき，任意の有限生成左 $\mathfrak{R}$ 加群も極大条件（$\mathfrak{R}$ 部分加群について）を満たす．極小条件についても同様である．

証明　§4.1 問 4.4（の Σ 群に対する一般化）を用いる：N を Σ 群 G の Σ 正規部分群とするとき，G が Σ 部分群について極大条件を満たすためには，G/N および N がそれぞれ Σ 部分群について極大条件を満たすことが必要十分である．さて補題を V の生成元の最小個数 n に関する数学的帰納法によって証明しよう．$n=1$ ならば，$V=\mathfrak{R}v_1$ ($\exists v_1 \in V$) となり V は $\mathfrak{R}$ の剰余加群に同型であるから，$\mathfrak{R}$ が極大条件を満たせば，上の注意により V も極大条件を満たす．$V=\langle v_1, v_2, \cdots, v_n\rangle$ ($n>1$) としよう．$U=\langle v_1, v_2, \cdots, v_{n-1}\rangle$ とおけば，

$$V = U+\mathfrak{R}v_n, \qquad V/U \simeq \mathfrak{R}v_n/U\cap\mathfrak{R}v_n$$

である．第2式の右辺は上の注意により極大条件を満たし，数学的帰納法の仮定により U も極大条件を満たすから，再び最初の注意により，V が極大条件を満たすことがわかる．▌

補題 4.5 および Krull-Remak-Schmidt の定理からつぎの定理が得られる．

定理 4.7　$\mathfrak{R}$ を左イデアルについて極大条件，極小条件を満たす環とする．有限生成 $\mathfrak{R}$ 加群 V は直既約な $\mathfrak{R}$ 部分加群の直和に分解し，その分解は V の自己同型を無視して一意的である．とくに $\mathfrak{R}$ 自身直既約な左イデアルの直和に $\mathfrak{R}$ の自己同型を無視して一意的に分解する．——

なお，§4.2 補題 4.2 により，直既約分解の可能性だけならば，$\mathfrak{R}$ が極大条件を満たすことを仮定すれば十分である．また定理 4.5′ は環に対してつぎの定理を与える：

定理 4.8　環 $\mathfrak{R}$ に対してつぎの条件は同値である：

(i)　$\mathfrak{R}$ は左イデアルについて極大条件を満たす，

(ii)　$\mathfrak{R}$ の任意の左イデアルは有限生成である．

系　主イデアル整域 $\mathfrak{R}$ はイデアルについて極大条件を満たす．すなわち第3章補題 3.5 が成り立つ．——

最後に第3章で残されていた定理 3.12 の証明をしよう．

$\mathfrak{R}$ を主イデアル整域とする．V が有限生成 $\mathfrak{R}$ 加群で

$$V \simeq \mathfrak{R}/\langle e_1\rangle \oplus \mathfrak{R}/\langle e_2\rangle \oplus \cdots \oplus \mathfrak{R}/\langle e_r\rangle \qquad (e_1 | e_2 | \cdots | e_r,\ e_i \neq 0,\ \mathfrak{R} \neq \langle e_i\rangle)$$

のとき，イデアル $\langle e_1\rangle, \langle e_2\rangle, \cdots, \langle e_r\rangle$ の一意性をいえばよい．まず，$e_1 | e_2 | \cdots | e_r$ により

$$e_r v = 0 \qquad (\forall v \in V)$$

であるから，V は剰余環 $\overline{\mathfrak{R}} = \mathfrak{R}/\langle e_r\rangle$ の上の有限生成加群とみることができる．さらに§3.5の(3.15)により，V は

(＊) $$V \simeq \mathfrak{R}/\langle p_1^{b_1}\rangle \oplus \cdots \oplus \mathfrak{R}/\langle p_u^{b_u}\rangle \qquad (p_i \text{ は } p_i | e_r \text{ なる } \mathfrak{R} \text{ の素元})$$

の形に書け，イデアル $\langle p_1^{b_1}\rangle, \cdots, \langle p_u^{b_u}\rangle$ の一意性をいえばよいのであった．ところで，$\mathfrak{R}$ が主イデアル整域であることからつぎのことが容易にわかる：

(α) 剰余環 $\overline{\mathfrak{R}} = \mathfrak{R}/\langle a\rangle$ $(0 \neq a \in \mathfrak{R})$ は極大条件，極小条件を満たす，

(β) $\mathfrak{R}/\langle p^b\rangle$ (p は $\mathfrak{R}$ の素元，$0 < b \in \boldsymbol{Z}$) は直既約 $\mathfrak{R}$ 加群である．

問 4.11 上の(α), (β)を示せ．——

以上により上の(＊)は極大・極小条件を満たす環 $\overline{\mathfrak{R}} = \mathfrak{R}/\langle e_r\rangle$ 上の有限生成加群 V の直既約分解を与えることがわかった．したがって Krull-Remak-Schmidt の定理によりイデアル $\langle p_1^{b_1}\rangle, \langle p_2^{b_2}\rangle, \cdots, \langle p_u^{b_u}\rangle$ は一意的でなければならない(§3.5問3.9参照)．

第5章 交 換 子

本章では交換子について述べる．交換子は群の構造を調べる上に大切な役割を果たす．われわれは第2章§2.4でそのような例をすでに見て来たのであった．§5.1では交換子の性質を，§5.2では可解群とともに群論における基本概念の一つである巾(べキ)零群の性質を説明する．§5.3で群のFitting部分群と成分について述べる．これらは近年有限群論において重要な役割を果たすようになってきた．

§5.1 交 換 子

群 G の二つの元 x, y に対して，$x^{-1}y^{-1}xy$ を x と y の**交換子**といい，

$$[x, y] = x^{-1}y^{-1}xy$$

と書く．以後つぎの記法が便利なので用いる：

$$x^y = y^{-1}xy \qquad (x, y \in G).$$

このとき

$$(xy)^z = x^z y^z, \qquad [x, y] = x^{-1}x^y \qquad (x, y, z \in G)$$

が成り立つ．交換子のつぎの性質は，定義から直接に確かめられる：

(5.1) $\qquad [x, y] = 1 \Leftrightarrow xy = yx,$

(5.2) $\qquad [x, y]^{-1} = [y, x],$

(5.3) $\qquad [x, y]^z = [x^z, y^z],$

(5.4) $\qquad [xy, z] = [x, z]^y[y, z], \qquad [x, yz] = [x, z][x, y]^z.$

問 5.1 (5.1)-(5.4) を確かめよ．——

群 G の部分集合 H, K に対して

$$[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle$$

とおく．$\langle \cdots \rangle$ は … で生成される G の部分群を表わす．したがって $[H, K]$ は交換子 $[h, k]$ $(h \in H,\ k \in K)$ によって生成される G の部分群である．とくに

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle$$

を G の**交換子群**という．$[G, G]$ はしばしば $D(G)$ と書かれる：

$$D(G) = [G, G].$$

例 5.1 G が Abel 群ならば, $D(G)=1$ である. 逆も成り立つ.

例 5.2 k を体とする. $D(GL_n(k))=SL_n(k)$, $D(SL_n(k))=SL_n(k)$ である. ただし $(n, |k|) \neq (2,2), (2,3)$ とする. $GL_n(k) \ni x, y$ に対して $x^{-1}y^{-1}xy$ の行列式は 1 だから, $D(GL_n(k)) \subseteqq SL_n(k)$ である. 第2章§2.4 ですでに見たように, $D(SL_n(k))=SL_n(k)$ だから, $D(GL_n(k))=SL_n(k)$ を得る.

例 5.3 $D(\mathfrak{S}_n)=\mathfrak{A}_n\,(n \geqq 3)$, $n \geqq 5$ のときには $D(\mathfrak{A}_n)=\mathfrak{A}_n$. なぜならば, $\mathfrak{S}_n \ni \sigma, \tau$ に対して $\sigma^{-1}\tau^{-1}\sigma\tau$ は偶置換だから, $D(\mathfrak{S}_n) \subseteqq \mathfrak{A}_n$. 第2章§2.4 で見たように $D(\mathfrak{A}_n)=\mathfrak{A}_n$ $(n \geqq 5)$. よって $n \geqq 5$ のときには $D(\mathfrak{S}_n)=\mathfrak{A}_n$. $n=3, 4$ のときには $D(\mathfrak{S}_n)=\mathfrak{A}_n$ となることを読者自ら確かめよ.

補題 5.1 H, K を G の部分群とする.

(i) $[H, K] = [K, H] \lhd \langle H, K \rangle$.

(ii) $H \subseteqq N_G(K) \Leftrightarrow [H, K] \subseteqq K$.

(iii) $G \rhd H,\ G \rhd K \Longrightarrow [H, K] \subseteqq H \cap K,\ [H, K] \lhd G$.

証明 (i) $[H, K]=[K, H]$ は (5.2) から出る. $H \ni h, h'$, $K \ni k, k'$ とすると (5.4) から

$$[h, k]^{h'} = [hh', k][h', k]^{-1} \in [H, K],$$
$$[k, h]^{k'} = [kk', h][k', h]^{-1} \in [K, H] = [H, K]$$

である. これは, $\langle H, K \rangle \rhd [H, K]$ を示す.

(ii) $N_G(K)=\{g \in G \mid g^{-1}Kg=K\}$ であった(問1.11参照). $H \subseteqq N_G(K)$ ならば, $H \ni h$, $K \ni k$ に対して

$$h^{-1}k^{-1}h \in h^{-1}Kh = K$$

である. よって $[h, k]=(h^{-1}k^{-1}h)k \in K$, すなわち $[H, K] \subseteqq K$ である. 逆に $[H, K] \subseteqq K$ とする. $H \ni h$, $K \ni k$ に対して, $[h, k]=h^{-1}k^{-1}hk \in K$ であるから, $h^{-1}k^{-1}h \in K$. すなわち $h^{-1}Kh=K$ である.

(iii) $G \rhd K$ ならば, $H \subseteqq G=N_G(K)$. (ii)により $[H, K] \subseteqq K$. 同様に $G \rhd H$ より, $H \supseteqq [K, H]=[H, K]$. よって $[H, K] \subseteqq H \cap K$. (5.3) により $[H, K] \lhd G$ である. ▌

問 5.2 $G \supseteqq H \rhd K$ (H は G の部分群)とする. $L=\{x \in G \mid [x, H] \subseteqq K\}$ とおく.

(i) $L \subseteqq N_G(H) \cap N_G(K)$.

(ii) L は G の部分群である.

問 5.3 $G \supseteqq H \supseteqq K$ (H, K は G の部分群)とする. $[G, H] \subseteqq K$ ならば, H, K は G の正規部分群で H/K は G/K の中心に含まれる. ——

つぎの補題は交換子群の基本性質である.

補題 5.2 (i) $G \triangleright D(G)$.

(ii) $G \triangleright N$, $G/N = \text{Abel}$ 群 $\Longleftrightarrow N \supseteqq D(G)$.

証明 (i)は補題5.1の(iii)から明らかである. (ii) $G \triangleright N$ のとき $x, y \in G$ に対して

(*) $(xN)(yN) = (yN)(xN) \Longleftrightarrow xyN = yxN \Longleftrightarrow x^{-1}y^{-1}xy \in N$

である. したがって G/N が Abel 群ならば, 任意の x, y に対して $[x, y] \in N$ すなわち $D(G) \subseteqq N$. 逆に $D(G) \subseteqq N$ とすると, 任意の x, y に対して $[x, y] \in N$. とくに $x \in N$ とすると, $y^{-1}xy \in xN = N$, よって $y^{-1}Ny \subseteqq N$. したがって $N \triangleleft G$ である. このとき(*)から G/N は Abel 群である. ▌

一般に群 G の G に始まり単位群に終る部分群の有限列

$$G = G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1$$

で,

(5.5) $\qquad G_{i-1} \triangleright G_i, \quad G_{i-1}/G_i = \text{Abel 群} \qquad (i=1, 2, \cdots, n)$

なるものが存在するとき, G を可解群というのであった(第2章§2.4). (5.5)は補題5.2の(ii)により

(5.5)′ $\qquad [G_{i-1}, G_{i-1}] \subseteqq G_i \qquad (i=1, 2, \cdots, n)$

と同値である. 各 i に対して

(5.6) $\qquad [G, G_{i-1}] \subseteqq G_i \qquad (i=1, 2, \cdots, n)$

を満たす部分群の列 $G = G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1$ が存在するとき G を**巾零群**という. 問5.3により(5.6)は G_{i-1}/G_i が G/G_i の中心に含まれることと同値である. このとき G_{i-1}/G_i は Abel 群だから, 巾零群は可解群である.

§5.2 可解群と巾零群

この節では可解群と巾零群の基本性質を調べよう. 群 G に対してその部分群 $D_i(G)$ $(i=0, 1, 2, \cdots)$ をつぎのように定義する:

(5.7) $\qquad D_0(G) = G, \quad D_i(G) = [D_{i-1}(G), D_{i-1}(G)] \qquad (i=1, 2, \cdots)$.

とくに $D_1(G)=D(G)=[G,G]$ である．明らかに $D_{i-1}(G)\supseteqq D_i(G)$ であり，また補題5.1の(iii)により $D_i(G)$ は G の正規部分群である．一般に G の部分群 H が G の任意の自己同型で不変のとき，H を G の**特性部分群**という(第4章§4.1,c)参照)．$D_i(G)$ は G の特性部分群であることは容易にわかる．

問5.4 これを確かめよ．

問5.5 群 G の正規部分群の特性部分群は，G の正規部分群であることを示せ．

補題5.3 つぎの条件は同値である：

(i) G は可解群である，

(ii) 或る n に対して $D_n(G)=1$.

証明 (i) $\Longrightarrow$ (ii)：G は可解群であるから，(5.5)′ により

$$G_i \supseteqq [G_{i-1}, G_{i-1}] \qquad (i=1,2,\cdots,n)$$

を満たす部分群の列 G_i が存在する．このとき，

$$G_i \supseteqq D_i(G) \qquad (i=1,2,\cdots,n) \tag{5.8}$$

を示そう．$i=0$ のときは明らかに成り立つ．$G_{i-1}\supseteqq D_{i-1}(G)$ と仮定すると (5.5)′ および(5.7)により

$$G_i \supseteqq [G_{i-1}, G_{i-1}] \supseteqq [D_{i-1}(G), D_{i-1}(G)] = D_i(G).$$

$G_n=1$ だから，(5.8)から $D_n(G)=1$ を得る．

(ii) $\Longrightarrow$ (i)：$D_n(G)=1$ のとき，$G_i=D_i(G)$ $(i=1,2,\cdots,n)$ とおけば G_i 達は明らかに(5.5)′ を満たす．▌

例5.4 可解群の実例のいくつかについては，第2章§2.4で述べた．ここでもう一つ実例をあげよう．k を任意の体として，k の元を成分とする n 次上半三角行列

$$\begin{bmatrix} a_1 & & * \\ & a_2 & \\ & & \ddots & \\ 0 & & & a_n \end{bmatrix} \qquad (a_i \neq 0)$$

の全体の作る群を $T(n)$ で表わす．$T_i(n)$ を

$$\begin{bmatrix} \overbrace{1 \ \ 0 \ \cdots \ 0}^{i} & & & & * \\ & 1 & 0 & \cdots & 0 & \ddots \\ & & \ddots & \ddots & & 0 \\ & & & \ddots & \ddots & \vdots \\ & & & & \ddots & 0 \\ 0 & & & & & 1 \end{bmatrix}$$

なる形の行列全体からなる $T(n)$ の部分群とする．このとき，

(5.9)　　$D_i(T(n)) \subseteq T_i(n)$　　$(i=1, 2, \cdots, n)$

である．$T_n(n)=1$ だから，$T(n)$ は可解群である．

問 5.6　(5.9) を証明せよ．

補題 5.4　H を G の部分群とする．

(i)　$D_i(G) \supseteqq D_i(H)$ $(i=1, 2, \cdots)$．とくに G が可解群ならば H も可解群である．

(ii)　$G \triangleright H$ ならば，$D_i(G/H)=D_i(G)H/H$．とくに G が可解群ならばその剰余群も可解群である．——

この証明は容易であるから読者にまかせる．

例題 5.1　有限可解群の極小正規部分群は，或る素数に対する基本 Abel 群である．

[証明]　N を有限可解群の極小正規部分群とする．補題 5.4 により N も可解群だから $N \neq D(N)$．$D(N)$ は N の特性部分群だから問 5.5 により $D(N) \triangleleft G$．N の極小性により $D(N)=1$，すなわち N は Abel 群である．$|N|$ を割る素数 p を一つとり

$$N_0 = \{x \in N \mid x^p=1\}$$

とおくと，N_0 は N の特性部分群である．再び問 5.5 により $N_0 \triangleleft G$．$N_0 \neq 1$ だから，N の極小性により $N=N_0$ である．これは N が基本 Abel 群であることを示す．▌

G の部分群 $K_i(G)$ $(i=0, 1, 2, \cdots)$ をつぎのように定義する：

(5.10)　　$K_0(G) = G$,　　$K_i(G) = [G, K_{i-1}(G)]$　$(i=1, 2, \cdots)$.

明らかに $K_{i-1}(G) \supseteqq K_i(G)$ であり，また補題 5.1 を用いて $G \triangleright K_i(G)$ がわかる．

さらに $K_i(G)$ は G の特性部分群であることが容易にわかる．いま構成した部分群の列

$$G = K_0(G) \supseteqq K_1(G) \supseteqq K_2(G) \supseteqq \cdots$$

を G の**降中心列**という．もちろん或る n に対して $K_n(G)=K_{n+1}(G)\neq 1$ なることがある．つぎに G の部分群 $Z_i(G)$ を

(5.11) $\qquad Z_0(G) = 1, \qquad Z_i(G) = \{x \in G \mid [x, G] \subseteqq Z_{i-1}(G)\} \qquad (i=1, 2, \cdots)$

によって定義すれば，問5.2により $G \triangleright Z_i(G)$，$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$ ($Z(\cdots)$ は $\cdots$ の中心を表わす）であり，とくに $Z_1(G)$ は G の中心 $Z(G)$ にほかならない．部分群の列

$$1 = Z_0(G) \subseteqq Z_1(G) \subseteqq \cdots$$

を G の**昇中心列**という．もちろん或る n に対して $Z_n(G)=Z_{n+1}(G)\neq G$ になることがある．

補題 5.5 つぎの条件は同値である：

(i) G は巾零群，

(ii) 或る n に対して $K_n(G)=1$，

(iii) 或る m に対して $Z_m(G)=G$.

証明 G を巾零群とすると，G は (5.6) により

$$[G, G_{i-1}] \subseteqq G_i \qquad (i=1, 2, \cdots, n)$$

なる性質をもつ部分群の列 $G=G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1$ をもつ．このとき各 i に対して，

(5.12) $\qquad K_i(G) \subseteqq G_i, \qquad G_{n-i} \subseteqq Z_i(G) \qquad (i=1, 2, \cdots, n)$

であることを示そう．$i=0$ のときは明らかに成り立つ．$K_{i-1}(G) \subseteqq G_{i-1}$ と仮定すると

$$K_i(G) = [K_{i-1}(G), G] \subseteqq [G_{i-1}, G] \subseteqq G_i$$

である．また $G_{n-i+1} \subseteqq Z_{i-1}(G)$ とすると，

$$[G_{n-i}, G] \subseteqq G_{n-i+1} \subseteqq Z_{i-1}(G)$$

となり，(5.12) が成り立つ．さて $G_0=G$，$G_n=1$ だから (5.12) により $K_n(G)=1$，$Z_n(G)=G$ を得る．すなわち (i) から (ii), (iii) が証明された．逆に (ii) または (iii) が成り立つとき，それぞれ $K_i(G)=G_i$ または $Z_{m-i}(G)=G_i$ とおけば部分群の列 G_i は (5.6) を満たすから，G は巾零である．▌

補題5.5の証明からつぎのことがわかる：G を巾零群とすると，

(5.13) $$Z_n(G) = G \Leftrightarrow K_n(G) = 1.$$

$Z_n(G)=G$ となる最小の整数 n を巾零群 G の**巾零クラス**あるいは簡単に**クラス**という．

例 5.5 Abel 群はクラス1の巾零群ということにほかならない．

例 5.6 p 群は巾零群である．G を p 群とすると，定理2.4により $Z(G)\neq 1$. $G/Z(G)$ も p 群だから $Z(G/Z(G))=Z_2(G)/Z(G)\neq 1$，すなわち $Z_1(G)\subsetneqq Z_2(G)$. 同様に $Z_2(G)\subsetneqq Z_3(G)$. これを続けて或る n に対して $Z_n(G)=G$ となるから，補題5.5により G は巾零群である．

例 5.7 $T_i(n)$ を例5.4の通りとすると，

$$[T_1(n), T_{i-1}(n)] \subseteqq T_i(n) \qquad (i=1, 2, \cdots, n)$$

が容易に確かめられる．よって $T_1(n)$ は巾零群である．

問 5.7 G を巾零クラスが高々2の巾零群とする．このときつぎの(i), (ii)を示せ：

(i) $[xy, z] = [x, z][y, z], \quad [x, yz] = [x, y][x, z]$,

(ii) $(xy)^n = x^n y^n [y, x]^{n(n-1)/2}$.

問 5.8 $T_{i+1}(n)=K_i(T_1(n))=Z_{n-i}(T_1(n))$ を示せ．

問 5.9 $\mathfrak{S}_3, \mathfrak{S}_4$ は可解群であるが，巾零群でないことを確かめよ．

補題 5.6 H を G の部分群とする．

(i) $K_i(G)\supseteqq K_i(H)$ $(i=0, 1, 2, \cdots)$. とくに巾零群の部分群は巾零群である．

(ii) $G\triangleright H$ のとき，$K_i(G/H)=K_i(G)H/H$. とくに巾零群の剰余群は巾零群である．——

この証明は全く容易であるから読者にまかせる．

問 5.10 補題5.6において $K_i(\cdots)$ の代わりに $Z_i(\cdots)$ をとったとき同じことが成り立つか．——

つぎの定理は巾零群のもっとも大切な性質である．

定理 5.1 H を巾零群 G の真の部分群とする：$G\supsetneqq H$. このときつぎの(i), (ii)が成り立つ：

(i) $N_G(H) \supsetneqq H$,

(ii) $G \triangleright H \neq 1$ のとき $[G, H] \subsetneqq H, \quad H\cap Z(G) \neq 1$.

証明
$$G=G_0 \supseteqq G_1 \supseteqq \cdots \supseteqq G_{n-1} \supseteqq G_n = 1,$$
$$[G, G_{i-1}] \subseteqq G_i \qquad (i=1,2,\cdots,n)$$
とする．$H \supseteqq G_i$ なる最小の i を l とする：
$$H \supseteqq G_l, \qquad H \not\supseteqq G_{l-1}.$$
このとき，
$$[G_{l-1}, H] \subseteqq [G_{l-1}, G] \subseteqq G_l \subseteqq H$$
となり，これは補題5.1の(ii)により $G_{l-1} \subseteqq N_G(H)$ を示す．$H \not\supseteqq G_{l-1}$ だから $H \subsetneqq N_G(H)$ である．よって(i)が証明された．つぎに $G \triangleright H \neq 1$ としよう．今度は $G_i \supseteqq H$ なる最大の i をとりそれを l とする：$G_l \supseteqq H$, $G_{l+1} \not\supseteqq H$. このとき，
$$[H, G] \subseteqq [G_l, G] \subseteqq G_{l+1}.$$
一方，$G \triangleright H$ より $[H,G] \subseteqq H$ である．よって
$$[H, G] \subseteqq H \cap G_{l+1} \subsetneqq H$$
を得る．$H_0 = H$, $H_i = [H_{i-1}, G]$ $(i=1,2,\cdots)$ とすると，いま示したことを H_i に適用して
$$H_0 \supsetneqq H_1 \supsetneqq \cdots \supsetneqq H_m = 1, \qquad H_i \triangleleft G$$
を得る．このとき $1 \neq H_{m-1} \subseteqq Z(G) \cap H$ である．▌

つぎの定理は，有限群が巾零群であるための必要十分条件を与える．

定理 5.2　G を有限群とする．G が巾零群であるためには，各素数に対する Sylow 部分群が G の正規部分群であることが必要十分である．このとき G は各素数に対する Sylow 部分群の直積となる．——

このことは定理5.1とつぎの補題から出る．

補題 5.7　G を有限群，P を素数 p に対する G の Sylow 部分群とすると，$N_G(N_G(P)) = N_G(P)$ である．

証明　$H = N_G(P)$ とおく．$N_G(H) \ni x$ とすると $x^{-1}Px \subseteqq H$ で $x^{-1}Px$ は P とともに H の Sylow p 部分群である．したがって Sylow の定理2.3により，$y \in H$ が存在して $x^{-1}Px = y^{-1}Py$ である．このとき $xy^{-1} \in N_G(P) = H$, よって $x \in H$ となる．これは $N_G(H) \subseteqq H$, したがって $N_G(H) = H$ を示す．▌

定理 5.2 の証明　G を巾零群，P を G の Sylow p 部分群とする．$N_G(P) \neq G$ ならば定理5.1により $N_G(N_G(P)) \supsetneqq N_G(P)$ となり，これは補題5.7に反する．よって $N_G(P) = G$, すなわち $P \triangleleft G$ となる．逆に，各素数 p に対して Sylow p

部分群を G の正規部分群としよう．$p_1, p_2, \cdots, p_n$ を G の位数を割る素数，P_i を Sylow p_i 部分群とすると

$$G \rhd P_i,$$
$$G = P_1P_2\cdots P_n,$$
$$P_i \cap (P_{i+1}P_{i+2}\cdots P_n) = 1 \qquad (i=1, 2, \cdots, n-1)$$

である．これは第4章問4.6により $G=P_1\otimes P_2\otimes\cdots\otimes P_n$ を示す．P_i は例5.6により巾零群だから，下の問5.11を用いれば，G が巾零群であることがわかる．▌

定理5.2により有限巾零群の構造は p 群の構造を調べることに帰着されることがわかる．

問5.11　$G=G_1\otimes G_2\otimes\cdots\otimes G_n$ とする（G は無限群でもよい）．このとき，つぎの(i), (ii)が成り立つ：

(i)　$D_i(G)=D_i(G_1)\otimes D_i(G_2)\otimes\cdots\otimes D_i(G_n)$．とくに各 G_i が可解群ならば，G は可解群である，

(ii)　$K_i(G)=K_i(G_1)\otimes K_i(G_2)\otimes\cdots\otimes K_i(G_n)$．とくに各 G_i が巾零群ならば，G は巾零群である．——

つぎに進むために高階の交換子を定義しよう．$G\ni x_1, x_2, \cdots, x_n$ $(n\geqq 2)$ に対して帰納的に

$$[[x_1, x_2, \cdots, x_{n-1}], x_n] = [x_1, x_2, \cdots, x_n]$$

によって n 階交換子 $[x_1, x_2, \cdots, x_n]$ を定義する．$n=2$ のときが普通の交換子である．同様に G の部分集合 $S_1, S_2, \cdots, S_n$ $(n\geqq 2)$ に対して

$$[[S_1, S_2, \cdots, S_{n-1}], S_n] = [S_1, S_2, \cdots, S_n]$$

によって G の部分群 $[S_1, S_2, \cdots, S_n]$ を定義する．明らかに

$$[S_1, S_2, \cdots, S_n] \supseteqq \langle [s_1, s_2, \cdots, s_n] \mid s_i\in S_i\rangle$$

であるが，一般には等号が成立するとは限らない．しかし，$G\rhd H_i$ $(i=1, 2, \cdots, n)$ ならば

(5.14)　$[H_1, H_2, \cdots, H_n] = \langle [h_1, h_2, \cdots, h_n] \mid h_i\in H_i\rangle,$

(5.15)　$[H_1, H_2, \cdots, H_n] \subseteqq [H_{i_1}, H_{i_2}, \cdots, H_{i_r}] \qquad (1\leqq i_1\leqq i_2\leqq\cdots\leqq i_r\leqq n)$

であることが，(5.4)と補題5.1を用いて容易に確かめられる．

問5.12　(5.14), (5.15)を確かめよ．——

$G\ni x, y, z$ に対して

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1 \tag{5.16}$$

なる恒等式が成り立つ．これを **Witt の恒等式**という．

問 5.13 (5.16) を確かめよ．——

つぎの補題は便利である．

補題 5.8(3 部分群補題) H, K, L を G の部分群，N を G の正規部分群とするとき，

$$[H, K, L] \subseteqq N, \quad [K, L, H] \subseteqq N \Longrightarrow [L, H, K] \subseteqq N.$$

証明 $H \ni x,\ K \ni y,\ L \ni z$ のとき，仮定により $[x, y^{-1}, z] \in N$，$[y, z^{-1}, x] \in N$．よって (5.16) により $[z, x^{-1}, y] \in N$．これは $[L, H]$ の生成元が K の各元と $\bmod N$ で交換可能であることを意味するから，$[L, H]$ と K が $\bmod N$ で元別に交換可能，すなわち $N \supseteqq [[L, H], K] = [L, H, K]$ を得る．▌

補題 5.9 $G \triangleright N_i\ (i=0, 1, 2, \cdots, r)$, $N_0 \supseteqq N_1 \supseteqq \cdots \supseteqq N_r$ とする．$[L, N_i] \subseteqq N_{i+1}\ (i=0, 1, 2, \cdots, r-1)$ ならば，$[K_j(L), N_i] \subseteqq N_{i+j+1}$.

証明 j に関する数学的帰納法による．$j=0$ のときは補題の仮定により成り立つ．また数学的帰納法の仮定により，

$$[K_{j-1}(L), N_i, L] \subseteqq [N_{i+j}, L] \subseteqq N_{i+j+1},$$
$$[N_i, L, K_{j-1}(L)] \subseteqq [N_{i+1}, K_{j-1}(L)] \subseteqq N_{i+j+1}$$

であるから，3 部分群補題を用いて

$$[K_j(L), N_i] = [L, K_{j-1}(L), N_i] \subseteqq N_{i+j+1}$$

を得る．▌

定理 5.3 (i) $[K_i(G), K_j(G)] \subseteqq K_{i+j+1}(G)$.

(ii) G が巾零群ならば，$[K_i(G), Z_{i+1}(G)] = 1$.

証明 (i) 補題 5.9 において $L=G,\ N_i=K_i(G)$ とすればよい．

(ii) $G=Z_n(G) \supsetneqq Z_{n-1}(G) \supsetneqq \cdots \supsetneqq Z_1(G) \supsetneqq Z_0(G)=1$ を G の昇中心列とするとき，$L=G,\ N_i=Z_{n-i}(G)\ (i=0, 1, 2, \cdots, n)$ とおいて補題 5.9 を適用すればよい．▌

問 5.14 G をクラス n の巾零群とする．m を $n/2$ をこえない最大の整数とするとき，$K_m(G)$ は Abel 群である．

§5.3 Fitting 部分群と成分

まず群の巾零正規部分群の性質を調べよう．

補題 5.10 N_1, N_2 を G の巾零正規部分群とするとき，その積 N_1N_2 も巾零正規部分群である．

証明 一般に $G \triangleright A, B, C$ のとき，(5.4)によって

$$[AB, C] = [A, C][B, C], \qquad [A, BC] = [A, B][A, C]$$

であることに注意する．このことと i に関する数学的帰納法を用いて

$$(5.17) \qquad K_i(N_1N_2) = \langle [L_1, L_2, \cdots, L_{i+1}] \mid L_j = N_1 \text{ または } N_2 \rangle$$

であることが容易にわかる．N_1, N_2 の巾零クラスをそれぞれ n_1, n_2 とする．$[L_1, L_2, \cdots, L_{n_1+n_2+1}]$ ($L_j = N_1$ または N_2) の中に N_1 が少なくとも n_1+1 回現われるか N_2 が少なくとも n_2+1 回現われるかのいずれかであるから，それに応じて (5.15)から

$$[L_1, L_2, \cdots, L_{n_1+n_2+1}] \subseteqq [\underbrace{N_1, N_1, \cdots, N_1}_{n_1+1}] \text{ または } [\underbrace{N_2, N_2, \cdots, N_2}_{n_2+1}]$$

を得る．右辺は N_1, N_2 の巾零クラスが n_1, n_2 であることから単位群である．したがって(5.17)により $K_{n_1+n_2}(N_1N_2)=1$. ▌

G が正規部分群について極大条件を満たすとき，補題5.10により G はただ一つの極大巾零正規部分群をもつことがわかる．これを G の **Fitting 部分群** といい，$F(G)$ と書く．$F(G)$ のつぎの性質は興味深い．

定理 5.4 G が正規部分群について極大極小条件を満たすとして，

$$G = G_0 \supsetneqq G_1 \supsetneqq \cdots \supsetneqq G_{n-1} \supsetneqq G_n = 1$$

を G の主組成列とする．このとき，

$$F(G) = \bigcap_{i=1}^{n} C_G(G_{i-1}/G_i)$$

である．ここで $C_G(G_{i-1}/G_i) = \{x \in G \mid [x, G_{i-1}] \subseteqq G_i\}$ である．

証明 N を G の巾零正規部分群とする．$\bar{G} = G/G_i$, $\bar{N} = NG_i/G_i$ とおく．$N \subseteqq C_G(G_{i-1}/G_i)$ を見るには $[\bar{N}, \bar{G}_{i-1}] = 1$ を示せばよい．$\bar{N} \neq 1$ としてよい．$\bar{N} \cap \bar{G}_{i-1} = 1$ ならば，$[\bar{N}, \bar{G}_{i-1}] \subseteqq \bar{N} \cap \bar{G}_{i-1} = 1$ となる．$\bar{N} \cap \bar{G}_{i-1} \neq 1$ ならば，$\bar{G}_{i-1}$ が $\bar{G}$ の極小正規部分群であるから $\bar{N} \cap \bar{G}_{i-1} = \bar{G}_{i-1}$ すなわち $\bar{N} \supseteqq \bar{G}_{i-1}$. $\bar{G}_{i-1} \neq 1$ だから，定理5.1(ii)により $Z(\bar{N}) \cap \bar{G}_{i-1} \neq 1$. $Z(\bar{N}) \cap \bar{G}_{i-1} \triangleleft \bar{G}$ および $\bar{G}_{i-1}$ の極小性により $Z(\bar{N}) \cap \bar{G}_{i-1} = \bar{G}_{i-1}$ すなわち $Z(\bar{N}) \supseteqq \bar{G}_{i-1}$. よって $[\bar{N}, \bar{G}_{i-1}] = 1$ を得る．とくに $N = F(G)$ にいままでのことを適用すれば，

$$F(G) \subseteq \bigcap_{i=1}^{n} C_G(G_{i-1}/G_i)$$

を得る．$D=\bigcap_{i=1}^{n} C_G(G_{i-1}/G_i)$ とおく．逆の包含関係を見るためには，$D \lhd G$ は明らかであるから D が巾零群であることをいえばよい．D の定義により $[D, G_{i-1}] \subseteq G_i\ (i=1, 2, \cdots, n)$ である．したがって補題5.9から $[K_{n-1}(D), G] \subseteq G_n=1$, すなわち $K_{n-1}(D) \subseteq Z(G)$. よって，

$$K_n(D) = [D, K_{n-1}(D)] \subseteq [D, Z(G)] = 1.$$

これは D が巾零群であることを示す．▌

以下では群 G の交換子群 $D(G)=[G, G]$ を簡単に G' で表わすことにしよう．群 G が

(5.18)　$G = G'$　かつ　$G/Z(G) =$ 単純群

なる条件を満たすとき，G を**準単純群**という．また G が

(5.19)　$G = G'$　かつ　$G/Z(G) =$ 単純群の直積

であるとき，G を**半単純群**という．(5.18), (5.19)において現われる単純群は，非可換単純群であることに注意する．なお，便宜上単位群を準単純群，半単純群の仲間に入れることにしよう．

補題 5.11　$G/Z(G)$ が非可換単純群の直積ならば，G' は半単純群である．

証明　$Z=Z(G)$, $\bar{G}=G/Z$ とおく．仮定により $\bar{G}$ は非可換単純群の直積だから $\bar{G}'=\bar{G}$ (問5.11(i))．補題5.4の(ii)により $\bar{G}'=\overline{G'}$. よって $\bar{G}=\overline{G'}$ すなわち $G=G'Z$. これから $Z(G')=G' \cap Z(G)$, $G/Z=G'Z/Z \simeq G'/Z \cap G'=G'/Z(G')$. また $G=G'Z$ の両辺の交換子群をとって $G'=G''(=[G', G'])$. よって G' は半単純群である．▌

以下の議論で3部分群補題をしばしばつぎの形で用いる：

G の部分群 H, K に対して

(5.20)　$[H, K, K] = 1 \Longrightarrow [H, K'] = 1,$

(5.21)　$[H, K] \subseteq Z(K),\quad K = K' \Longrightarrow [H, K] = 1.$

問 5.15　(5.20), (5.21)を確かめよ．——

半単純群のつぎの性質は大切である．

補題 5.12　G を半単純群とするとき，

(i)　$G = G_1 G_2 \cdots G_n,$

(ii) $G_i=$ 準単純群 $\neq 1$,

(iii) $[G_i, G_j]=1 \quad (i\neq j)$

なる条件を満たす $G_1, G_2, \cdots, G_n$ が一意的に定まる．逆に G が(i), (ii), (iii)を満たせば，G は半単純群である．

証明 $Z=Z(G)$，$\bar{G}=G/Z$ とおく．半単純群の定義により

$$\bar{G}=\bar{G}_1\otimes\bar{G}_2\otimes\cdots\otimes\bar{G}_n, \qquad \bar{G}_i=\text{非可換単純群}$$

である．G の正規部分群 X_1 で

(5.22) $$\bar{X}_1=\bar{G}_1, \qquad X_1=X_1' \qquad (\text{ただし } \bar{X}_1=X_1Z/Z)$$

を満たすものがただ一つ存在する．実際 $G\triangleright Y_1$, $\bar{Y}_1=\bar{G}_1$ とすると，$\bar{Y}_1=\bar{G}_1=\bar{G}_1'=\bar{Y}_1'=\overline{Y_1'}$ だから $Y_1Z=Y_1'Z$．両辺の交換子群をとって $Y_1'=Y_1''$．よって Y_1' が(5.22)を満たす．また X_1, Y_1 がともに(5.22)を満たせば，$X_1Z=Y_1Z$．よって $X_1'=Y_1'$ すなわち $X_1=Y_1$ となる．(5.22)を満たす X_1 を G_1 と書こう．同様にして $G_2, G_3, \cdots, G_n$ を定義する．このとき $G=G_1G_2\cdots G_nZ$ であるが，両辺の交換子群をとって $G=G_1G_2\cdots G_n$ を得る．また $[\bar{G}_i, \bar{G}_j]=1$ $(i\neq j)$ より $[G_i, G_j]\subseteqq Z$．よって $[G_i, G_j, G_j]\subseteqq[Z, G_j]=1$．(5.20)により $1=[G_i, G_j']=[G_i, G_j]$．これから，$Z(G_i)=Z(G)\cap G_i$，$G_i/Z(G_i)=G_i/Z\cap G_i\simeq G_iZ/Z=\bar{G}_i=$単純である．以上により(i), (ii), (iii)を満たす $G_1, G_2, \cdots, G_n$ の存在が証明された．逆に $G_1, G_2, \cdots, G_n$ が(i), (ii), (iii)を満たせば $\bar{G}=G/Z$ は $\bar{G}_i=G_iZ/Z$ の直積で $G'=G$ であるから半単純である．また，$G_1, G_2, \cdots, G_n$ の一意性は，補題4.4(i)により $\bar{G}$ の直積因子が一意的であるから，(5.22)を満たす X_1 の一意性からわかる．▌

補題 5.13 E_1, E_2 が G の半単純正規部分群ならば，その積 E_1E_2 も G の半単純正規部分群である．

証明 $Z_i=Z(E_i)\,(i=1,2)$, $Z=Z_1Z_2$, $E=E_1E_2$ とおく．$G\triangleright E$ は明らかだから E が半単純群であることを示せばよい．そのためにまず $Z\subseteqq Z(E)$ を示そう．$Z_1\triangleleft G$, $E_2\triangleleft G$ より $[Z_1, E_2]\subseteqq Z_1\cap E_2$．$Z_1\cap E_2$ は半単純群 E_2 の可換正規部分群だから $Z_1\cap E_2\subseteqq Z_2$ である．よって $[Z_1, E_2]\subseteqq Z_2$．このとき(5.21)により $[Z_1, E_2]=1$ だから $Z_1\subseteqq Z(E)$ を得る．同様に $Z_2\subseteqq Z(E)$，したがって $Z=Z_1Z_2\subseteqq Z(E)$ である．$\bar{G}=G/Z$，$\bar{E}=E/Z$ とおく．$\bar{E}_i=E_iZ/Z\simeq E_i/E_i\cap Z=E_i/Z_i$ より $\bar{E}_i$ は非可換単純群の直積で $\bar{G}$ の正規部分群である．このとき補題4.4(ii)により $\bar{E}=\bar{E}_1\bar{E}_2$ も非可換単純群の直積となり，これから $Z=Z(E)$ を得る．したがって E は

半単純群となる. ▌

上の補題 5.13 により G が正規部分群について極大条件を満たせば, ただ一つの極大半単純正規部分群をもつことがわかる. これを $E(G)$ で表わす. $E(G)$ は明らかに G の特性部分群である. また $E(G)\neq 1$ のとき, $E(G)$ は補題 5.12 の (i), (ii), (iii) を満たす $E_1, E_2, \cdots, E_n$ の積であるが, これらの E_i を G の**成分**という. 正規部分群について極大条件を満たす G に対して,

$$F^*(G)=F(G)E(G)$$

とおくと,

$$[F(G), E(G)]=1 \tag{5.23}$$

である. 実際 $[F(G), E(G)]\subseteqq F(G)\cap E(G)\subseteqq Z(E(G))$ だから, (5.21) から, (5.23) を得る. $F^*(G)$ を G の**一般化された Fitting 部分群**ということがある. つぎの定理は $F^*(G)$ のもっとも大切な性質である.

定理 5.5 G を組成列をもつ群とするとき, $C_G(F^*(G))=Z(F(G))\subseteqq F^*(G)$ である. ——

証明にはつぎの補題を用いる.

補題 5.14 D は組成列をもつ群で $F(D)=Z(D)$ とする. このとき D は Abel 群であるかあるいは $E(D)\neq 1$.

証明 $\bar{D}=D/Z(D)$ も組成列をもつから補題 4.4(iii) により, $\bar{D}$ は極小正規部分群 $\bar{L}=L/Z(D)$ をもち, $\bar{L}$ は Abel 群または非可換単純群の直積である. $\bar{L}$ が Abel 群ならば L は D の巾零正規部分群となり, $L\subseteqq F(D)$. これは仮定 $F(D)=Z(D)$ に反する. したがって $\bar{L}$ は非可換単純群の直積となるから補題 5.13 により L' は D の半単純正規部分群となり $1\neq L'\subseteqq E(D)$ を得る. ▌

定理 5.5 の証明 $D=C_G(F^*(G))$ とおく. $E(D)$ は G の正規部分群 D の特性部分群だから G の正規部分群である. よって $E(D)\subseteqq E(G)$. D の定義により $[E(D), E(G)]=1$ だから $E(D)=1$ でなければならない. 同様の理由で $F(D)\subseteqq F(G)$ となる. これから $F(D)=Z(F(G))=Z(D)$ を得る. このとき補題 5.14 により D は Abel 群でなければならない. したがって $D=Z(D)=Z(F(G))$. ▌

定理 5.5 の特別な場合としてつぎの定理が成り立つ.

定理 5.6 G が有限可解群ならば $C_G(F(G))=Z(F(G))\subseteqq F(G)$ である.

補題 5.15 G を組成列をもつ群, H を G の部分群とする.

(i) L が G の成分ならば，$[L,H]=1$ または $L\subseteqq[L,H]$.

(ii) $E_1,E_2,\cdots,E_r$ を $[E_i,H]\neq1$ なる G の成分の全体とすると，$[E(G),H]=E_1E_2\cdots E_r$. とくに，$E(G)=[E(G),H]C_{E(G)}(H)$，$[E(G),H,H]=[E(G),H]$ である.

証明 $K\rightleftarrows[L,H]$ とおく．$K\subseteqq E(G)$，$L\lhd E(G)$ であるから，$N_G(L)\supseteqq K$ である．また補題5.1(i)により $N_G(K)\supseteqq L$. よって $[K,L]\subseteqq K\cap L\lhd L$. L は準単純群だから，$K\cap L=L$ または $K\cap L\subseteqq Z(L)$ である．$K\cap L=L$ ならば，$L\subseteqq[H,L]$ である．$K\cap L\subseteqq Z(L)$ ならば，$[K,L]\subseteqq Z(L)$. このとき，(5.21)により $[K,L]=1$. すなわち $[H,L,L]=1$ である．よって(5.20)により，$[H,L']=1$. しかるに $L'=L$ であるから，$[H,L]=1$ である．これで(i)が示された．$E(G)=E_1E_2\cdots E_n$，$[E_i,H]\neq1\,(1\leqq i\leqq r)$，$[E_j,H]=1\,(j>r)$ としよう．H は $E(G)$ の成分 $E_1,E_2,\cdots,E_n$ の上の置換をひき起すから，$E_1E_2\cdots E_r$ は H 不変，すなわち $[E_1E_2\cdots E_r,H]\subseteqq E_1E_2\cdots E_r$ である．一方(i)により $E_i\subseteqq[E_i,H]\,(1\leqq i\leqq r)$ である．よって，

$$E_i\subseteqq[E_i,H]\subseteqq[E(G),H]=[E_1E_2\cdots E_r,H]\subseteqq E_1E_2\cdots E_r,$$

$$E_1E_2\cdots E_r=[E(G),H]=[E_1E_2\cdots E_r,H].$$

これから，$E(G)=[E(G),H]C_{E(G)}(H)$，$[E(G),H,H]=[E(G),H]$ を得る．∎

第6章　自　由　群

本章では自由群とそれに関連した事項について説明する．自由群の重要性は，生成元とその間の関係式によって群を定義したり，そのような群を取り扱う上の基礎を与える点にある．§6.1で自由群の定義，存在，一意性などを示し，§6.2では有限生成自由群の部分群に関するSchreierの定理を証明する．§6.3では，任意の群が生成元とそれらの基本関係によって定義されることを示し，いくつかの具体的な群に対して生成元とその基本関係式を与える．

§6.1　自 由 群

a）定義，存在，一意性

集合 S に対して S の濃度を $|S|$ で表わす．まず自由群の定義を与えよう．

定義 6.1　F を群，S を F の部分集合とする．つぎの条件が満たされるとき，F を S 上の**自由群**，S を F の**自由生成系**という：

(6.1)　S は F の生成系である：$F=\langle S\rangle$,

(6.2)　G を $|T|\leqq|S|$ なる生成系 T をもつ任意の群とする：

$$G=\langle T\rangle,\qquad |T|\leqq|S|.$$

このとき，S から T の上への任意の全射 φ に対して F から G の上への準同型 f が存在して $f(s)=\varphi(s)$ $(\forall s\in S)$ となる．いいかえると S から T への全射が F から G の上への準同型に延長される．——

簡単にいえば，自由群とは一定の濃度の生成系をもつ群の中でもっとも一般的なものである．F が S 上の自由群のとき，S の濃度 $|S|$ を F の**階数**という．つぎの意味で S 上の自由群 F の一意性が成り立つ．なお，つぎの定理の逆である階数の一意性については定理6.2を参照されたい．

定理 6.1　F_i を S_i 上の自由群とする $(i=1,2)$．$|S_1|=|S_2|$ ならば F_1 と F_2 は同型である．

証明　φ を S_1 から S_2 の上への任意の全単射とする．定義の条件(6.2)から，φ は F_1 から F_2 の上への準同型 f に延長される．φ の逆写像 φ^{-1} も S_2 から S_1

の上への全単射だから，同様の理由でそれは F_2 から F_1 の上への準同型 g に延長される．このとき

$$f\circ g=1_{F_2}, \quad g\circ f=1_{F_1} \quad (1_{F_i} \text{ は } F_i \text{ の恒等写像})$$

であるから，f は F_1 から F_2 の上への同型である．▌

つぎに，任意の集合 S に対して S 上の自由群が存在することを示そう．$S=\{s_\lambda \mid \lambda\in\Lambda\}$ (Λ は添数集合) とする．S の元 s_λ に対して記号 s_λ^{-1} を定め，s_λ^{-1} の全体を S^{-1} とおく．($|S'|=|S|$, $S\cap S'=\phi$ なる集合 S' および S から S' への全単射 φ をとり $\varphi(s_\lambda)=s_\lambda^{-1}$ とおくといってもよい.)

$$S_0=S\cup S^{-1} \qquad (S\cap S^{-1}=\phi)$$

とおく．S_0 の有限個の元の(重複)順列(それを積の形で書く)

$$s_1s_2\cdots s_n \qquad (s_i\in S_0,\ 0<n\in \boldsymbol{Z})$$

を S 上の**語**という．また空順列も考えてそれを**空語**という．空語は1で表わされる．S 上の語全体(空語も含めて)を W で表わす．$W\ni w, w'$, $w=s_1s_2\cdots s_p$, $w'=s_1's_2'\cdots s_q'$ ($s_i, s_j'\in S_0$) に対して，それらの積を

$$ww'=s_1s_2\cdots s_ps_1's_2'\cdots s_q' \tag{6.3}$$

と定義する．空語1に対しては

$$1w=w1=w \qquad (\forall w\in W) \tag{6.4}$$

である．この積は明らかに結合法則を満たすから，W は単位元1をもった半群である．さて W の上に補題1.2の条件を満たす同値関係を定義しよう．$W\ni w_1, w_2$, $w_1=s_1s_2\cdots s_p$ のとき，w_2 が

$$w_2=s_1s_2\cdots s_{i-1}(tt^{-1})s_i\cdots s_p{}^{1)} \qquad (t\in S_0)$$

の形をしているならば，$w_1\to w_2$ と書く．さらに $w_1=w_2$, $w_1\to w_2$, $w_2\to w_1$ のいずれかが成り立つとき，$w_1\approx w_2$ と書こう．さらに $W\ni w, w'$ に対して $W\ni w_0, w_1, \cdots, w_n$ が存在して，

$$w=w_0, \quad w'=w_n, \quad w_i\approx w_{i+1} \quad (i=0,1,2,\cdots,n-1)$$

のとき，$w\sim w'$ と書く．この関係 $w\sim w'$ は明らかに W 上の同値関係である．この同値関係はつぎの性質(6.5), (6.6)をもつ：

$$w_1\sim w_1', \quad w_2\sim w_2' \Longrightarrow w_1w_2\sim w_1'w_2', \tag{6.5}$$

1) $t\in S^{-1}$, $t=s^{-1}$ ($s\in S$) のとき $t^{-1}=s$ とする．

(6.6) $W \ni \forall w, \quad W \ni \exists w', \quad ww' \sim 1.$

$u \approx v$ のとき任意の $w \in W$ に対して $wu \approx wv$, $uw \approx vw$ であることが $\approx$ の定義から明らかであるから，これを繰返し用いて $w_1 w_2 \sim w_1' w_2 \sim w_1' w_2'$，すなわち(6.5)が成り立つ．(6.6)は $w = s_1 s_2 \cdots s_p$ のとき，$w' = s_p^{-1} s_{p-1}^{-1} \cdots s_1^{-1}$ とすればよい．

$W \ni w$ に対して w を含む同値類を $[w]$ で表わそう．(6.5), (6.6)はこの同値関係が補題1.2の条件を満たすことを示している．したがって補題1.2により商集合 $F = W/\sim$ は，

(6.7) $$[w_1][w_2] = [w_1 w_2]$$

なる積に関して群となる．以下，いま構成された群 F が S の上の自由群であることを示そう．まず，S の異なる二つの元は同値でないから $s \in S$ と $[s]$ を同一視することにより S を F の部分集合と考えることにする．このとき S が F の生成系であることは明らかである．つぎに条件(6.2)を試そう．G, T, φ を(6.2)におけるようにとる．$\varphi(s_\lambda^{-1}) = \varphi(s_\lambda)^{-1}$ とおくことにより，φ は S_0 から $T \cup T^{-1}$ の上への全射をひき起す．この全射も φ で表わそう．$W \ni w = s_1 s_2 \cdots s_n$ $(s_i \in S_0)$ に対して $\varphi(s_1)\varphi(s_2)\cdots\varphi(s_n) \in G$ を対応させる W から G への写像 f を考える：

$$f(s_1 s_2 \cdots s_n) = \varphi(s_1)\varphi(s_2)\cdots\varphi(s_n).$$

$w \approx w'$ ならば，明らかに $f(w) = f(w')$ だから，

$$w \sim w' \Longrightarrow f(w) = f(w')$$

となる．したがって f は F から G への写像 $\bar{f}$:

(6.8) $$\bar{f}([w]) = f(w)$$

を誘導する．また明らかに

(6.9) $$f(w_1 w_2) = f(w_1) f(w_2) \qquad (w_1, w_2 \in W)$$

であるから，(6.7), (6.8), (6.9)により

$$\bar{f}([w_1][w_2]) = \bar{f}([w_1])\bar{f}([w_2])$$

となる．これは，$\bar{f}$ が F から G への準同型であることを示す．さらに $\bar{f}([s]) = f(s) = \varphi(s)$ $(s \in S)$ であるから，$\bar{f}$ は(6.2)を満たす．以上によって F は S 上の自由群であることが示された．

b）語の簡約表示

S を任意の集合，W を S 上の語の集合とする．$W \ni w = s_1 s_2 \cdots s_n$ $(s_i \in S_0 = S \cup S^{-1})$ が各 i に対して $s_{i+1} \neq s_i^{-1}$ のとき，w は**簡約されている**あるいは**簡約語**で

あるという．空語1も簡約語と約束する．

補題6.1　W の各同値類はただ一つの簡約語を含む．

証明　$W\ni w=s_1s_2\cdots s_n$ に対してつぎのような簡約語の列 $w_0, w_1, \cdots, w_n$ を作る操作を考える．まず

$$w_0=1, \quad w_1=s_1$$

として，w_i をつぎのように帰納的に定める：$w_{i-1}=s_1's_2'\cdots s_t'$ のとき

$$w_i=\begin{cases} s_1's_2'\cdots s_{t-1}' & (s_t'=s_i^{-1} \text{ のとき}), \\ s_1's_2'\cdots s_t's_i & (s_t'\neq s_i^{-1} \text{ のとき}) \end{cases}$$

とおく．これを簡単にいうと，$w=s_1s_2\cdots s_n$ を最初の項から順番に‘簡約していく’操作を考えているわけである．この操作で最終的に得られる簡約語 w_n を $r(w)$ で表わすことにしよう．このとき，

(6.10)　$$w\sim r(w),$$

(6.11)　$$w \text{ が簡約語 } \Longrightarrow w=r(w)$$

であることは明らかである．(6.10)は各同値類が少なくとも一つの簡約語を含むことを示している．さて

(6.12)　$$w\approx w' \Longrightarrow r(w)=r(w')$$

を示そう．$w=s_1s_2\cdots s_n$，$w'=s_1s_2\cdots s_{i-1}(tt^{-1})s_i\cdots s_n$ のそれぞれに対して上のように簡約語の列

$$w_0,\ w_1,\ \cdots,\ w_n,$$
$$w_0',\ w_1',\ \cdots,\ w_n',\ w_{n+1}',\ w_{n+2}'$$

を作る．$j\leqq i-1$ のとき $w_j=w_j'$ であることは明らかである($i-1$ 番目までの操作は w, w' の両者に対して全く同一である)．つぎに $w_{i-1}=w_{i+1}'$ を示そう．w_{i-1} の最終項が t^{-1} すなわち $w_{i-1}'=w_{i-1}=w_{i-2}t^{-1}$ ならば，$w_i'=w_{i-2}$，$w_{i+1}'=w_{i-2}t^{-1}=w_{i-1}$ となり，また w_{i-1} の最終項が t^{-1} でなければ，$w_i'=w_{i-1}t$, $w_{i+1}'=w_{i-1}$ であるから，いずれの場合も $w_{i-1}=w_{i+1}'$ となる．このとき，w_{i-1} から $w_i, w_{i+1}, \cdots w_n$ を作る操作と，w_{i+1}' から $w_{i+2}', \cdots, w_{n+2}'$ を作る操作は全く同一となるから，結局 $w_n=w_{n+2}'$ すなわち $r(w)=r(w')$ を得る．したがって(6.12)が示された．(6.12)から

(6.13)　$$w\sim w' \Longrightarrow r(w)=r(w')$$

が得られることは明らかである．(6.13)において w, w' がともに簡約語ならば，

(6.11)を用いて $w=r(w)=r(w')=w'$ を得る．これで補題は証明された．▌

以下では S 上の語は，S 上の自由群 $F=W/\sim$ の元を表わすと考えるのが便利である．もちろん同値な語は F の同一の元を表わすわけである．このとき，補題6.1は F の各元が簡約語で表わされ，異なる簡約語は F の異なる元を表わすことを主張している．いいかえると F の各元 $s\neq 1$ は，

$$s = s_1^{n_1}s_2^{n_2}\cdots s_r^{n_r} \qquad (s_i\in S,\ 0\neq n_i\in \boldsymbol{Z},\ s_i\neq s_{i+1})$$

の形に一意的に書き表わせることがわかった．

つぎの補題は，或る群 G とその生成系 X が与えられたとき，G が X 上の自由群であるための簡単な判定条件を与える．

補題 6.2 $G=\langle X\rangle$ とする．このときつぎの条件は同値である：

(i) G は X 上の自由群である，

(ii) G の各元 $x(\neq 1)$ は

$$x = x_1^{n_1}x_2^{n_2}\cdots x_r^{n_r} \qquad (x_i\in X,\ 0\neq n_i\in \boldsymbol{Z},\ x_i\neq x_{i+1})$$

の形に一意的に書き表わせる，

(iii) $X\cap X^{-1}=\phi$．また $X\cup X^{-1}\ni x_1, x_2, \cdots, x_n$，$x_ix_{i+1}\neq 1\ (i=1, 2, \cdots, n-1)$ ならば $x_1x_2\cdots x_n\neq 1$．

証明 (i) $\Longrightarrow$ (ii)：これは上に述べた．(ii) $\Longrightarrow$ (iii) は明らかである．(iii) $\Longrightarrow$ (i) を証明しよう．F を S 上の自由群で $|S|=|X|$ とする．φ を S から X への全単射とすると φ は F から G の上への準同型に延長される．φ が同型であることを示すために $F\ni w\neq 1$，$\varphi(w)=1$ と仮定して矛盾を出そう．$w=s_1s_2\cdots s_n$ を w の簡約表示(すなわち w は簡約語)とすると，$\varphi(s_i)=x_i\in X$ とおいて

$$1 = \varphi(w) = \varphi(s_1)\varphi(s_2)\cdots\varphi(s_n) = x_1x_2\cdots x_n$$

である．仮定(ii)により或る i に対して

$$x_ix_{i+1} = 1 \quad すなわち \quad x_{i+1} = x_i^{-1}$$

である．一方，$X\cap X^{-1}=\phi$ より φ は $S\cup S^{-1}$ から $X\cup X^{-1}$ の上への全単射であるから，$s_{i+1}=s_i^{-1}$．これは $w=s_1s_2\cdots s_n$ が簡約表示であることに反する．したがって，$\varphi(w)=1$ ならば $w=1$ となり φ は F から G の上への同型である．▌

つぎに自由群の階数の一意性を示してこの節を終ろう．

定理 6.2 S, T を自由群 F の自由生成系とするとき，$|S|=|T|$ である．

証明 $S=\{s_\lambda\mid\lambda\in\Lambda\}$ とする．S から $\{1, -1\}$ の上への写像は，(6.2)により F

から位数2の群 $\{1,-1\}$ の上への準同型をひき起し，その核は F の指数2の部分群である．逆に F の指数2の部分群を与えると S から $\{1,-1\}$ の上への準同型が定まる．したがって F の指数2の部分群の全体と S から $\{1,-1\}$ への全射の全体とは1対1に対応する．$|S|=r<\infty$ ならば，このような全射は 2^r-1 個あるから，いま述べたことから $|S|=|T|$ でなければならない．また $|S|=\infty$ ならば $|T|=\infty$ である．ところで $|S|=\infty$ のとき，補題6.2の(ii)からわかるように $|S|=|F|$，よって $|S|=|T|$ を得る．▌

§6.2 自由群の性質

自由群とくに有限生成自由群については，いろいろな興味あることが知られている．この節では，その一つとして，Schreier の定理を証明しよう．

定理 6.3 (Schreier) H を自由群 F の部分群とする．このときつぎが成り立つ：

(i) H も自由群である，

(ii) F の階数が $r\,(<\infty)$ で，$[F:H]=n$ ならば，H の階数は $1+n(r-1)$ である．——

この定理の証明は本節の最後で与えられる．F を自由群，S をその自由生成系としよう．$F\ni x$, $x=s_1s_2\cdots s_n$ $(s_i\in S_0=S\cup S^{-1})$ を x の簡約表示とするとき，$l(x)=n$ とおき $l(x)$ を x の(S に関する)**長さ**という．また F の部分集合 T がつぎの条件(S)を満たすとき，S に関して **Schreier の性質**をもつという：

(S) $T\ni t=s_1s_2\cdots s_n$ が簡約されているとき，$s_1s_2\cdots s_{n-1}\in T$.

補題 6.3 H を自由群 F の部分群とする．H の右剰余類の代表系 T で(S)を満たすものが存在する．

証明 H の各剰余類 Hx に対して，Hx に含まれる元の長さの最小値を Hx の長さといい，$l(Hx)$ と書こう．明らかに $l(H)=0$ である．さて各整数 $n\geqq 0$ に対してつぎの性質をもつ F の部分集合 T_n を構成しよう：

(α) $T_n\ni s \Longrightarrow l(s)=n$,

(β) T_n は長さ n の H の右剰余類の代表系である，

(γ) $T_n\ni t=s_1s_2\cdots s_n$ が簡約されているとき，$s_1s_2\cdots s_{n-1}\in T_{n-1}$.

n に関する数学的帰納法による．$n=0$ のとき $T_0=\{1\}$ である．$T_0, T_1, \cdots, T_{n-1}$

まで構成されたものとしよう．Hx を長さ n の右剰余類とする．$l(x)=n$ としてよい．$x=s_1s_2\cdots s_n$ を x の簡約表示として $x'=s_1s_2\cdots s_{n-1}$ とおけば，$n-1=l(x')=l(Hx')$ である．よって(β)により $Hx'=Ht'$ なる $t'\in T_{n-1}$ が存在する．このとき $t=t's_n$ とおけば $l(t)=n$, $Hx=Ht$, $t'\in T_{n-1}$ である．長さ n の各右剰余類からこのように代表系 t を選んで，それらの集合を T_n とおけば，T_n は(α), (β), (γ)を満たしている．このとき $T=\bigcup_{n=0}^{\infty}T_n$ とおけば，T が性質(S)をもつことはあきらかであろう．▌

F, S, H, T を補題6.3のようにとる．F の各元 x は $x=ht$ $(h\in H,\ t\in T)$ と一意的に書けるから，F から H への写像 η と F から T への写像 τ を

$$\eta(x)=h, \qquad \tau(x)=t$$

によって定義する．このとき，

$$\eta(ts)=ts\cdot\tau(ts)^{-1} \qquad (t\in T,\ s\in S_0=S\cup S^{-1}), \tag{6.14}$$

$$TST^{-1}\cap H=\{\eta(ts)\,|\,t\in T,\ s\in S\} \tag{6.15}$$

が成り立つ．さらに補題1.5により $TST^{-1}\cap H$ は H の生成系である．$TST^{-1}\cap H$ の単位元でない元の全体を Y とおく：

$$Y=\{\eta(ts)\neq 1\,|\,t\in T,\ s\in S\}.$$

Schreier の定理の証明の要点は，Y が H の自由生成系であることを示すことにある．そのために $\eta(ts)=ts\cdot\tau(ts)^{-1}$ の簡約表示をくわしく調べる必要がある．まず(6.14)から $\eta(ts)^{-1}=\tau(ts)s^{-1}t^{-1}$ であるから $\eta(\tau(ts)s^{-1})=\eta(ts)^{-1}$ である．ここで(s をとめて)t を T 全体を動かすと，$\tau(ts)$ も T 全体を動くから

$$Y^{-1}=\{\eta(ts^{-1})\neq 1\,|\,t\in T,\ s\in S\}$$

となる．したがって $Y_0=Y\cup Y^{-1}$ とおけば

$$Y_0=\{\eta(ts)\neq 1\,|\,t\in T,\ s\in S_0=S\cup S^{-1}\}$$

である．

F の元の列 $x_1, x_2, \cdots, x_n$ は，それぞれの簡約表示をそのまま並べて作った積が，$x_1x_2\cdots x_n$ の簡約表示になっているとき，$x_1, x_2, \cdots, x_n$ の間に**簡約は起らない**ということにしよう．

補題 6.4 $Y_0\ni\eta(ts)=ts\cdot\tau(ts)^{-1}$ $(t\in T,\ s\in S_0)$ とする．このとき $t, s, \tau(ts)^{-1}$ の間に簡約は起らない．また $Y_0\ni\eta(t_1s_1)=\eta(t_2s_2)$ ならば，$t_1=t_2$, $s_1=s_2$ である．

証明 $t, s, \tau(ts)^{-1}$ の間に簡約が起るとすると，t の簡約表示の終項が s^{-1} であ

るか，$\tau(ts)^{-1}$ の簡約表示の初項が s^{-1} のいずれかである．t の終項が s^{-1} ならば T の性質(S)により $ts\in T$．よって $\tau(ts)=ts$，すなわち $\eta(ts)=1$ となり，$Y_0\not\ni 1$ に反する．s^{-1} が $\tau(ts)^{-1}$ の初項すなわち s が $\tau(ts)$ の終項ならば，再び(S)により $\tau(ts)s^{-1}\in T$．よって $t=\eta(ts)\tau(ts)s^{-1}$ より $t=\tau(\tau(ts)s^{-1})=\tau(ts)s^{-1}$，すなわち $\eta(ts)=1$ となり矛盾である．したがって補題の前半が証明された．つぎに $Y_0\ni\eta(t_1s_1)=\eta(t_2s_2)$ ならば，$t_1s_1\cdot\tau(t_1s_1)^{-1}=t_2s_2\cdot\tau(t_2s_2)^{-1}$ だから簡約表示の一意性により $t_1=t_2$，$s_1=s_2$ でなければならない．▌

補題 6.5 $Y_0\ni y_i=\eta(t_is_i)\,(i=1,2)$ とする．$y_1y_2\neq 1$ ならば $t_1, s_1, \tau(t_1s_1)^{-1}t_2, s_2,$ $\tau(t_2s_2)^{-1}$ の間に簡約は起らない．

証明 補題6.4により t_1, s_1 と $s_2, \tau(t_2s_2)^{-1}$ の間に簡約は起らない．$\tau(t_1s_1)^{-1}t_2=1$，$s_1^{-1}=s_2$ ならば，$t_2s_1^{-1}t_1^{-1}=t_2s_2\cdot\tau(t_2s_2)^{-1}\in H$ より $t_1=\tau(t_2s_2)$．よって $y_1y_2=1$ となり矛盾である．したがって $\tau(t_1s_1)^{-1}t_2\neq 1$ としてよい．s_1 と $\tau(t_1s_1)^{-1}t_2$ の間に簡約が起るとすれば，補題6.4により t_2 の簡約表示は $\tau(t_1s_1)s_1^{-1}\cdots$ の形でなければならない．このとき(S)により $\tau(t_1s_1)s_1^{-1}\in T$．よって $\tau(t_1s_1)s_1^{-1}=\tau(\tau(t_1s_1)s_1^{-1})=t_1$，すなわち $y_1=\eta(t_1s_1)=1$ となり矛盾である．$\tau(t_1s_1)^{-1}t_2$ と s_2 の間に簡約が起るとすれば，再び補題6.4により $\tau(t_1s_1)$ の簡約表示は，$\tau(t_1s_1)=t_2s_2\cdots$ の形である．このとき(S)により $t_2s_2\in T$ すなわち $y_2=\eta(t_2s_2)=1$ となり矛盾である．▌

さて Schreier の定理6.3の証明を始めよう．

定理 6.3 の証明 はじめに定理6.3の(i)を示すためには，補題6.2により

$$Y_0\ni y_1, y_2, \cdots, y_n,\quad y_iy_{i+1}\neq 1\ \ (i=1,2,\cdots,n-1) \Longrightarrow y_1y_2\cdots y_n\neq 1,$$
$$Y\cap Y^{-1}=\phi$$

をいえばよい．$y_i=\eta(t_is_i)=t_is_i\cdot\tau(t_is_i)^{-1}$ とすると補題6.5により

$$t_1,\ s_1,\ \tau(t_1s_1)^{-1}t_2,\ s_2,\ \cdots,\ s_{n-1},\ \tau(t_{n-1}s_{n-1})^{-1}t_n,\ s_n,\ \tau(t_ns_n)^{-1}$$

の間に簡約は起らない．とくに $y_1y_2\cdots y_n$ の簡約表示に $s_1, s_2, \cdots, s_n$ が現われるから $y_1y_2\cdots y_n\neq 1$ である．つぎに $Y\cap Y^{-1}\ni y$ とすると，$y=\eta(t_1s_1)=\eta(t_2s_2^{-1})$ $(t_i\in T,\ s_i\in S)$ と書けるから，補題6.4の後半から $s_1=s_2^{-1}\in S\cap S^{-1}$ となり $S\cap S^{-1}=\phi$ に反する．したがって $Y\cap Y^{-1}=\phi$ である．よって定理6.3の(i)が証明された．つぎに定理6.3の(ii)を証明しよう．$|S|=r$，$[F:H]=n$ とおく．$Y_1=\{(t,s)\in T\times S_0\,|\,\eta(ts)=1\}$ とすると，補題6.4により

(6.16)　$$2|Y| = 2nr - |Y_1|$$

である．ところで

$$\eta(ts) = ts\cdot\tau(ts)^{-1} = 1 \iff \tau(ts) = ts$$

であるから，

(6.17)　$$(t, s) \in Y_1 \iff (ts, s^{-1}) \in Y_1$$

となり，Y_1 の元は (t, s), (ts, s^{-1}) なる対に分けることができる．このような対の個数を数えよう．(6.17) より $l(t) > l(ts)$ ならば s^{-1} は t の終項，$l(ts) > l(t)$ ならば s が ts の終項である．よって $Y_1 \ni (t, s)$，$l(t) > l(ts)$ のとき，s は t に対して一意的に定まり，しかも t として $t \neq 1$ なる任意の $t \in T$ がとれるから

$$|Y_1| = 2(n-1).$$

これと (6.16) から

$$|Y| = 1 + n(r-1)$$

を得る．すなわち H の階数は $1+n(r-1)$ である．▌

§6.3　生成元と関係式による群の定義

第1章例1.13，例1.14 において，生成系と関係式によって定義される群の実例を与えた．本節では，生成系と関係式によって群を定義する一般的原理を説明する．くわしくはつぎの結果が導かれる：

(6.18)　任意に与えられた関係を基本関係とする群が存在する，

(6.19)　任意の群とその任意の生成系が与えられたとき，生成系の基本関係式が存在する．——

S を任意の集合とする．S の濃度を r とする．(r は無限でもよいが記述を簡単にするため以下では r は有限であるかのごとき書き方をする.) S 上の語の集合

$$\mathcal{R} = \{R_\lambda(s_1, s_2, \cdots, s_r) \mid \lambda \in \Lambda\}$$

が与えられたとする．$\mathcal{R}$ を S 上の自由群 F の部分集合とみなし，$\mathcal{R}$ によって生成される F の正規部分群——すなわち $\mathcal{R}$ を含む F の最小の正規部分群——を N とする．$\bar{F} = F/N$ とおき，$x \mapsto \bar{x}$ を F から $\bar{F}$ への自然準同型とすれば，明らかにつぎの (6.20), (6.21) が成り立つ：

(6.20)　$$\bar{F} = \langle \bar{S} \rangle,$$

(6.21)　　　　$R_\lambda(\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_r) = 1 \qquad (\forall \lambda \in \Lambda).$

ここで大切なことは(6.21)が$\bar{F}$の生成系$\bar{S}$の基本関係式を与えることである.(基本関係式の定義については第1章§1.5参照.) 実際, $G=\langle T\rangle$, φが$\bar{S}$からTへの全射であって

(6.22)　　　　$R_\lambda(\varphi(\bar{s}_1), \varphi(\bar{s}_2), \cdots, \varphi(\bar{s}_r)) = 1 \qquad (\forall \lambda \in \Lambda)$

とすると, SからTへの全射($S \to \bar{S}$とφの合成写像)をFからGへの準同型ψに延長するとき, (6.22)は$\mathrm{Ker}\,\psi \supseteq N$を示す. よって$\bar{F}$から$G$への準同型$\bar{\varphi}$で$\bar{\varphi}(\bar{s}_1)=\psi(s_1)=\varphi(s_1)$なるものが存在する(問1.27参照). これは(6.21)が$\bar{S}$の基本関係式であることを示す. また以上で示したことは(6.18)が成り立つことを意味している.

つぎに(6.19)を示そう. Gを任意の群, XをGの生成系とする. $|S|=|X|$なる集合Sをとり, $S \ni s_i \mapsto x_i \in X$を$S$から$X$への全単射とする. このとき$s_i \mapsto x_i$は$S$上の自由群$F$から$G$の上への準同型に延長される. その核を$N$, Nの生成系を

$$\mathcal{R} = \{R_\lambda(s_1, s_2, \cdots, s_r) \mid \lambda \in \Lambda\}$$

とすると,

$$R_\lambda(x_1, x_2, \cdots, x_r) = 1 \qquad (\lambda \in \Lambda)$$

がGの生成系Xの基本関係式である. 実際, $H=\langle Y\rangle$, $x_i \mapsto y_i$がXからYの上への全射であって$R_\lambda(y_1, y_2, \cdots, y_r)=1$とすると, SからYへの全射$s_i \mapsto x_i \mapsto y_i$を$F$から$H$の上への準同型$\psi$に延長するとき$\mathrm{Ker}\,\psi \supseteq N$となり, これから問1.27により$G$から$H$の上への準同型で$x_i \mapsto y_i$なるものが存在することがわかる.

(6.18)は一般的原理として非常に具合のよいものではあるが, 与えられた関係式を基本関係式とする群がどんな群であるか(たとえば有限群であるか無限群であるかなど)をその関係から調べるのは一般には非常に難しい. またその群が単位群になってしまうこともある. たとえば, 2元a, bで生成され

$$b^3 = a^7 = 1, \quad b^{-1}ab = a^3, \quad a^{-1}ba = b^2$$

を基本関係とする群は単位群である. また最初の二つの関係

$$b^3 = a^7 = 1, \quad b^{-1}ab = a^3$$

から$a=1$が得られ, これらを基本関係とする群は位数3の巡回群である. 少し

変えて

$$b^3 = a^7 = 1, \quad b^{-1}ab = a^2$$

とすると，これは例1.14で与えた位数21の非 Abel 群 $\boldsymbol{Z}(7,3,2,0)$ となる．このように簡単な関係式でも少し変えると構造の全然違う群が生じるのである．

つぎに(6.19)について注意すると，その証明からも見られるように群と生成系に対して基本関係が一意的に定まるわけではない．一般には，なるべく形のよい，あるいは計算のしやすい基本関係を求めるのが望ましい．以下，対称群，交代群など具体的な群に対して生成系とその基本関係式の実例を与えよう．

例 6.1 $x^2=y^2=(xy)^n=1$ $(\boldsymbol{Z} \ni n>1)$ を基本関係とする群は位数 $2n$ の正2面体群 D_{2n} である．第1章例1.13によって D_{2n} は

$$a^n = b^2 = 1, \quad b^{-1}ab = a^{-1}$$

なる a, b によって生成されるのであった．

$$(ba)^2 = b^2 = 1, \quad (b \cdot ba)^n = 1$$

であるから，x, y によって生成される $x^2=y^2=(xy)^n=1$ を基本関係とする群を G とすれば，G から D_{2n} の上への準同型で $x \mapsto b$, $y \mapsto ba$ なるものが存在する．ところで $z=xy$ とおけば，

$$x^2 = z^n = 1, \quad x^{-1}zx = yx = z^{-1}, \quad G = \langle x, y \rangle = \langle x, z \rangle$$

より G の元は $x^i z^j$ $(0 \leqq i \leqq 1,\ 0 \leqq j \leqq n-1)$ と書けるから $|G| \leqq 2n$. よって G から D_{2n} の上への準同型は同型でなければならない．

例 6.2

$$\begin{aligned} &{x_1}^2 = {x_2}^2 = \cdots = {x_{n-1}}^2 = 1, \\ &(x_i x_{i+1})^3 = 1 \qquad (1 \leqq i \leqq n-2), \\ &(x_i x_j)^2 = 1 \qquad (|i-j|>1) \end{aligned}$$

を基本関係とする群 G_n は n 次対称群 $\mathfrak{S}_n$ と同型である．

［証明］ まず $\mathfrak{S}_n \ni y_i = (i\ \ i+1)$ $(1 \leqq i \leqq n-1)$ とすると，

$$\mathfrak{S}_n = \langle y_1, y_2, \cdots, y_{n-1} \rangle \qquad (\text{問 } 1.37 \text{ 参照})$$

であって，

$$\begin{aligned} &{y_1}^2 = {y_2}^2 = \cdots = {y_{n-1}}^2 = 1, \quad (y_i y_{i+1})^3 = 1, \\ &(y_i y_j)^2 = 1 \qquad (|i-j|>1) \end{aligned}$$

が容易に確かめられる．したがって G_n から $\mathfrak{S}_n$ の上への準同型 φ で $\varphi(x_i) = y_i$ $(1 \leqq i \leqq n-1)$ なるものが存在する．φ が G_n から $\mathfrak{S}_n$ の上への同型であることを

示そう．それには，$|G_n| \leqq n!$ であることを見れば十分である．このことを n に関する帰納法で示そう．$n=2$ のときは明らかに成り立つ．$H=\langle x_1, x_2, \cdots, x_{n-2}\rangle$ とおけば，帰納法の仮定により $|H| \leqq (n-1)!$ である．

$$H,\ Hx_{n-1},\ Hx_{n-1}x_{n-2},\ \cdots,\ Hx_{n-1}x_{n-2}\cdots x_1$$

なる H の n 個の右剰余類の和集合を K とする．各 x_i に対して $Kx_i=K$ を示せば $K \ni x_1, x_2, \cdots, x_{n-1}$ となり $G_n=K$. したがって $|G_n|=|K| \leqq |H|n \leqq n!$ となる．

$j>i+1$ とすると $x_ix_j=x_jx_i$, $H \ni x_i$ であるから

$$(Hx_{n-1}\cdots x_j)x_i = Hx_{n-1}x_{n-2}\cdots x_j \subseteqq K,$$

$j=i+1$ ならば，$(Hx_{n-1}\cdots x_j)x_i=Hx_{n-1}\cdots x_jx_i \subseteqq K$,

$j=i$ ならば，$(Hx_{n-1}\cdots x_j)x_i=Hx_{n-1}\cdots x_{i+1} \subseteqq K$,

$j<i$ ならば，$(Hx_{n-1}\cdots x_j)x_i=Hx_{n-1}\cdots x_{i+1}(x_ix_{i-1}x_i)x_{i-2}\cdots x_j$ において $x_ix_{i-1}x_i=x_{i-1}x_ix_{i-1}$ を用いて

$$\begin{aligned} Hx_{n-1}\cdots x_{i+1}(x_ix_{i-1}x_i)x_{i-2}\cdots x_j &= Hx_{n-1}\cdots x_{i+1}(x_{i-1}x_ix_{i-1})x_{i-2}\cdots x_j \\ &= Hx_{n-1}\cdots x_{i+1}x_ix_{i-1}\cdots x_j \end{aligned}$$

を得る．以上により $Kx_i=K\,(1 \leqq i \leqq n-1)$ となり，$|G_n| \leqq n!$ が得られた．▌

例 6.3 $n \geqq 3$ のとき，

$$\begin{aligned} &x_1{}^3 = x_2{}^2 = \cdots = x_{n-2}{}^2 = 1, \\ &(x_ix_{i+1})^3 = 1 \qquad (1 \leqq i \leqq n-3), \\ &(x_ix_j)^2 = 1 \qquad (j-i>1,\ i \geqq 1) \end{aligned}$$

を基本関係とする群 G_n は n 次交代群 $\mathfrak{A}_n$ と同型である．

［証明］ まず

$$y_1 = (1\ 2\ 3), \qquad y_{i-1} = (1\ 2)(i\ \ i+1) \quad (3 \leqq i \leqq n-1)$$

とおくと，

$$\mathfrak{A}_n = \langle y_1, y_2, \cdots, y_{n-2}\rangle \qquad (\text{問 1.45 参照})$$

であって

$$\begin{aligned} &y_1{}^3 = y_2{}^2 = \cdots = y_{n-2}{}^2 = 1, \qquad (y_iy_{i+1})^3 = 1, \\ &(y_iy_j)^2 = 1 \qquad (j-i>1,\ i \geqq 1) \end{aligned}$$

が容易に確かめられる．したがって G_n から $\mathfrak{A}_n$ への準同型 φ で $\varphi(x_i)=y_i$ $(1 \leqq i \leqq n-2)$ なるものが存在する．φ が同型であることを見るには $|G_n| \leqq n!/2$ を示せば十分である．$n=3$ のときは明らかに成り立つから，$H=\langle x_1, \cdots, x_{n-3}\rangle$,

$|H| \leqq (n-1)!/2$ と仮定しよう.

$$H,\ Hx_{n-2},\ Hx_{n-2}x_{n-3},\ \cdots,\ Hx_{n-2}x_{n-3}\cdots x_2x_1,\ Hx_{n-2}x_{n-3}\cdots x_2{x_1}^2$$

なる H の n 個の右剰余類の和集合を K として, 各 x_i に対して $Kx_i=K$ を示せば, $|G_n|=|K| \leqq |H|n \leqq n!/2$ を得る.

$$Hx_{n-2}x_{n-3}\cdots x_1x_i,\ Hx_{n-2}x_{n-3}\cdots {x_1}^2x_i \subseteqq K \qquad (i>1)$$

以外の関係は例6.2と同様に確かめられる. $i>2$ のとき $(x_1x_i)^2=1$ より $x_1x_i=x_i{x_1}^{-1}=x_i{x_1}^2$ であるから,

$$Hx_{n-2}x_{n-3}\cdots x_1x_i = Hx_{n-2}\cdots x_2x_i{x_1}^2$$

であり, 例6.2におけるのと同様にして

$$Hx_{n-2}\cdots x_2x_i = Hx_{n-2}\cdots x_2.$$

したがって,

$$Hx_{n-2}\cdots x_1x_i = Hx_{n-2}\cdots x_2{x_1}^2 \subseteqq K$$

を得る. 同様に $i>2$ のとき, $Hx_{n-2}\cdots {x_1}^2x_i=Hx_{n-2}\cdots x_2x_1 \subseteqq K$ である. $i=2$ ならば, $x_2x_1x_2={x_1}^2x_2{x_1}^2$ および $x_j{x_1}^2=x_1x_j$ $(j>2)$ を用いて

$$\begin{aligned}(Hx_{n-2}\cdots x_2x_1)x_2 &= Hx_{n-2}\cdots x_3{x_1}^2x_2{x_1}^2\\ &= Hx_{n-2}\cdots x_3x_2{x_1}^2 \subseteqq K\end{aligned}$$

である. 同様に $(Hx_{n-2}\cdots {x_1}^2)x_2=Hx_{n-2}\cdots x_1 \subseteqq K$. 以上により, 各 x_i に対して $Kx_i \subseteqq K$ が示された. ▌

例 6.4 q 個の元からなる有限体上の $n-1$ 次元特殊射影線型群 $PSL(n,q)$ と低い次数の交代群の間につぎの同型があることが知られている:

(i) $PSL(2,3) \simeq \mathfrak{A}_4$,

(ii) $PSL(2,4) \simeq PSL(2,5) \simeq \mathfrak{A}_5$,

(iii) $PSL(2,9) \simeq \mathfrak{A}_6$,

(iv) $PSL(4,2) \simeq \mathfrak{A}_8$.

これらの同型を確かめる方法はいくつか知られているが, 例6.3を利用するのがもっとも素朴である. まずつぎにあげる行列が例6.3の関係式を満たすこと(左から順番に $x_1, x_2, \cdots$ として)が直接の計算によって確かめられる(読者自ら試みよ). ただし行列 A に対して A と $-A$ は同一視しなければならない.

(i) $PSL(2,3)$; $\quad \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \quad \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}.$

(ii) $PSL(2,4)$; $\begin{bmatrix}\omega & 0\\ 0 & \omega^{-1}\end{bmatrix}$, $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$,

ω は4個の元からなる有限体 F_4 の乗法群の生成元である．したがって $\omega^3=1$, $\omega\neq 1$ である．

(iii) $PSL(2,9)$; $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$, $\begin{bmatrix}\iota & 1\\ 0 & \iota^{-1}\end{bmatrix}$, $\begin{bmatrix}\iota & 0\\ 0 & \iota^{-1}\end{bmatrix}$,

ι は F_9 の元で $\iota^2=-1$ なるものである．

(iv) $PSL(4,2)$; $\left[\begin{array}{cc|cc} & 1 & & \\ 1 & 1 & & \\ \hline & & & 1\\ & & 1 & 1\end{array}\right]$, $\left[\begin{array}{cc|cc}1 & & 1 & 1\\ & 1 & & 1\\ \hline & & 1 & \\ & & & 1\end{array}\right]$, $\left[\begin{array}{cc|cc} & & 1 & 1\\ & & & 1\\ \hline 1 & 1 & & \\ & 1 & & \end{array}\right]$,

$\left[\begin{array}{cc|cc}1 & 1 & 1 & 1\\ & 1 & & 1\\ \hline & & 1 & 1\\ & & & 1\end{array}\right]$, $\left[\begin{array}{cc|cc}1 & & & \\ 1 & 1 & & \\ \hline & & & 1\\ & & 1 & \end{array}\right]$, $\left[\begin{array}{cc|cc}1 & 1 & & \\ & 1 & & \\ \hline & & 1 & 1\\ & & & 1\end{array}\right]$.

ここであげた行列が例6.3の関係式を満たすことがわかれば，それぞれの場合に交代群からの全射準同型が得られる．(ii), (iii), (iv) のとき $\mathfrak{A}_5, \mathfrak{A}_6, \mathfrak{A}_8$ は単純群だからこの準同型は同型でなければならない．(i) の場合は，そこにあげた二つの行列が $PSL(2,3)$ を生成することが直接に確かめられるから，$\mathfrak{A}_4$ と $PSL(2,3)$ の位数を比べて $\mathfrak{A}_4\simeq PSL(2,3)$ を得る．なお，$PSL(2,5)$ に対して例6.3におけるような関係を満たす行列を求めることは読者にまかせる．実際は $PSL(2,5)$ の指数5の部分群（＝位数12の部分群）H の存在を示し，$PSL(2,5)$ の $PSL(2,5)/H$ 上の置換表現を考えることにより $PSL(2,5)\simeq\mathfrak{A}_5$ を示す方が自然である．興味のある読者は，この線に沿って $PSL(2,5)\simeq\mathfrak{A}_5$ の証明を試みられたい．なお $PSL(n,q)$ と $\mathfrak{A}_m$ の間には上にあげた同型以外には，同型が存在しないことも知られている[1)]．

例 6.5 $PSL(2,\boldsymbol{Z})$ を $SL(2,\boldsymbol{Z})$[2)] の中心 $\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$ による剰余群としよう．

---

1) E. Artin: The orders of the linear groups, Comm. Pure Appl. Math. 8(1955), 455–472.

2) $SL(2,\boldsymbol{Z})$ は I，p. 80 で $SL_2(\boldsymbol{Z})$ と書いた整数を成分とする行列式1の2次行列の作る群である．

$$x^2 = y^3 = 1$$

を基本関係とする群は，$PSL(2, \boldsymbol{Z})$ と同型である．

［証明］　問3.2により，$SL(2, \boldsymbol{Z})$ は，

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

なる二つの元で生成される．

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

であるから，$SL(2, \boldsymbol{Z})$ は，$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$ で生成され，これらはそれぞれ $PSL(2, \boldsymbol{Z})$ の位数 2, 3 の元である．したがって

$$G = \langle x, y \mid x^2 = y^3 = 1 \rangle$$

とすると，G から $PSL(2, \boldsymbol{Z})$ の上への準同型 φ が存在する．φ が同型であることを示そう．$x^2 = y^3 = 1$ だから，$\xi = xy$, $\eta = xy^{-1}$ とおくと，G の任意の元は ξ, η のいくつかの積あるいはそれらに x を右または左から掛けた形に書き表わせる．
ξ', η' を

$$\xi' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

$$\eta' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

なる $PSL(2, \boldsymbol{Z})$ の元とすると，φ の核の元の像 $(=1)$ を考えると，上の注意から

$$\xi' \equiv \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \eta' \equiv \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

のいくつかの積が

$$\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{または} \quad \pm \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

でなければならない．しかるに ξ', η' のいくつかの積の行列成分の和は明らかに 2 より大きいから，これは φ の核が 1 でなければならないことを示す．▌

問 6.1　可算無限個の生成元 $a_1, a_2, \cdots, a_n, \cdots$ によって生成され，${a_{n+1}}^{n+1} = a_n$ $(n = 1, 2, \cdots)$ を基本関係式とする群は有理数の加法群と同型である．

問 6.2　$G = \langle a, b \mid aba = bab \rangle$ とする．$x = ab^2$, $y = ab$ とおくと，

(i)　$x^2 = y^3 \in Z(G)$,

(ii) $G/Z(G) \simeq PSL(2, \boldsymbol{Z})$

を示せ.

問 6.3 $PSL(2, p)$ (p は素数)は, 位数 2, 位数 3 の二つの元で生成されることを示せ.

第7章　有　限　群

有限群の歴史は古く，したがって話題も多いが，ここでは最近の有限単純群論で使われている基本的な事柄を解説する．§7.1は準備である．§7.2では，Schur-Zassenhausの定理とその応用を述べる．§7.3では，いくつかのp巾零性定理を取り上げる．§7.2-§7.3の素材の多くは，むしろ古典的であるが，Alperinの定理7.12やThompsonのp巾零性定理7.15のように比較的新しい結果もある．また§7.2-§7.3の一つの具体的目標は，Thompsonの定理7.16——Frobenius群のFrobenius核の巾零性——の証明にある．§7.4では，最近の単純群論で重要な役割を果たしているp束縛性(p-constraint)，p安定性(p-stability)などの概念を説明する．§7.4, c)で述べるGlaubermanのZJ定理7.26は大切である．最後に§7.4, d)では，いわゆる2信号関手定理(Goldschmidtの定理)のBenderによる証明を紹介する．この2信号関手定理が応用上重要であることはもちろんであるが，その証明も最近の有限単純群論で用いられている方法を説明する簡単なモデルとみなすことができて興味深いものである．

§7.1　復習と準備

§7.1では，前章までに述べた有限群の主要性質の復習と§7.2-§7.4で必要な事柄の最小限の準備をする．

a) Sylowの定理とp群

当然のことながら，有限群論でもっとも基本的な定理は，Sylowの定理——定理2.3——である．pを素数とするとき有限群Gのp部分群Pでその指数$[G:P]$がpと素なものをGのSylow p部分群というのであった．以後Sylow p部分群を簡単にS_p**部分群**ということにしよう．GのS_p部分群全体の集合を$\mathrm{Syl}_p(G)$と書く．ここでSylowの定理を再録しておこう．

Sylowの定理　Gを有限群，pを素数とする．このときつぎが成り立つ：

(i)　Gは少なくとも一つのS_p部分群をもつ：$\mathrm{Syl}_p(G)\neq\phi$,

(ii)　$P\in\mathrm{Syl}_p(G)$，QをGの任意のp部分群とするとき，Qの或る共役はPに含まれる．とくに二つのS_p部分群は互いに共役である，

(iii)　$[G:N_G(P)]\equiv 1 \pmod p$　$(P\in\mathrm{Syl}_p(G))$,　$|\mathrm{Syl}_p(G)|\equiv 1 \pmod p$.

Sylowの定理のつぎの簡単な系は，本章で繰返し用いられる．なお，Gの部分集合Sと$G \ni x$に対して，Sの共役$x^{-1}Sx$をS^xと書く：

$$S^x = x^{-1}Sx.$$

補題 7.1 Gを有限群，pを素数とする．

(i) QがGの正規p部分群ならば，QはGの各S_p部分群に含まれる．とくにGの或るS_p部分群がGの正規部分群ならば，Gはただ一つのS_p部分群をもつ．

(ii) $G \triangleright N,\ \mathrm{Syl}_p(N) \ni P \Longrightarrow G = N_G(P)N.$

(iii) $G \triangleright N,\ P \in \mathrm{Syl}_p(G) \Longrightarrow N \cap P \in \mathrm{Syl}_p(N).$

証明 (i)はSylowの定理の(ii)の直接の結果である．(ii)を示そう．$G \ni x$とすると$P^x \subseteqq N^x = N$，よって$P^x \in \mathrm{Syl}_p(N)$．Sylowの定理により$N \ni y$が存在して$P^x = P^y$．したがって$xy^{-1} \in N_G(P)$，すなわち$x \in N_G(P)y \subseteqq N_G(P)N$である．$x$は$G$の任意の元だから，$G = N_G(P)N$を得る．(iii)を示す．$G \triangleright N$より$NP$は$G$の部分群である．このとき，$[NP:P] = [N:N \cap P]$．これから，(iii)がでる．▌

Sylowの定理から推察されるように，有限群論ではp群が大切な役割を演ずる．前章までに得られたp群の性質を思い起そう．Pをp群とするとき，

(α) Pは巾零群である．とくにその中心$Z(P)$は単位群ではない，

(β) $P \triangleright N \neq 1 \Longrightarrow N \cap Z(P) \neq 1$ （定理 5.1），

(γ) $P \supsetneqq Q \Longrightarrow N_P(Q) \supsetneqq Q$ （定理 5.1）．

(β), (γ)はもっと一般に有限巾零群の性質である．また有限巾零群は各素数pに対するS_p部分群達の直積であるから(定理 5.2)，有限巾零群の構造は完全にp群のそれを調べることに帰着される．上の(α), (β), (γ)のほかにもp群については，いろいろなことが知られているが，本書ではその一部を必要に応じてそのつど取り上げることにして，ここではp群のFrattini部分群についてふれるにとどめる．一般に有限群Gのすべての極大部分群の共通部分をGの**Frattini部分群**といい，$\Phi(G)$で表わす．Frattini部分群のつぎの簡単な性質は大切である．

補題 7.2 Sを有限群Gの部分集合とする．このとき，

$$G = \langle S, \Phi(G) \rangle \Longrightarrow G = \langle S \rangle.$$

証明 $G \neq \langle S \rangle$とする．$\langle S \rangle$を含む極大部分群Mをとると$\langle S \rangle \subseteqq M,\ \Phi(G) \subseteqq$

M だから，$G=\langle S, \Phi(G)\rangle=\langle S, M\rangle=\langle M\rangle=M$ となり矛盾である．▌

問 7.1 Frattini 部分群は巾零群である．［ヒント］補題 7.1 の (ii) と補題 7.2 の応用．

問 7.2 P が基本 Abel 群すなわち或る素数 p に対して $(p, p, \cdots, p)$ 型の群ならば，$\Phi(P)=1$. ——

本講では，Frattini 部分群を用いるのは p 群に対してだけである．

補題 7.3 P を p 群とする．

(i) $P \supsetneqq M$ が P の極大部分群 $\Leftrightarrow$ $[P:M]=p$. このとき $P \triangleright M$ である．

(ii) $P/\Phi(P)$ は基本 Abel 群である．とくに $\Phi(P) \supseteqq D(P)$ ($=P$ の交換子群).

(iii) $P \triangleright N$, $P/N=$ 基本 Abel 群 $\Leftrightarrow N \supseteqq \Phi(P)$.

証明 (i) M を P の極大部分群とする．上の (γ) により $N_P(M) \supsetneqq M$. よって M の極大性により $P=N_P(M)$. すなわち $P \triangleright M$. ふたたび M の極大性により P/M の位数は p でなければならない．(ii) $M_1, M_2, \cdots, M_r$ を P の指数 p の部分群の全体とする．(i) によりこれらは P の極大部分群の全体でもあるから $\Phi(P) =\bigcap_{i=1}^{r} M_i$. よって $P/\Phi(P)$ は基本 Abel 群 $P/M_1 \otimes \cdots \otimes P/M_1$ の部分群と同型となるから，$P/\Phi(P)$ も基本 Abel 群である．これから (iii) の $\Longleftarrow$ は明らかである．最後に (iii) の $\Longrightarrow$ であるが，上の問 7.2 により N を含む P の極大部分群全体の共通部分は N であることから $N \supseteqq \Phi(P)$ を得る．▌

一般に有限群 G と素数 p が与えられたとき

(i) G が指数 p ベキの正規部分群をもつための条件，

(ii) G が位数 p ベキの正規部分群をもつための条件

を G の S_p 部分群との関係 (S_p 部分群の構造とか，それの G への埋め込まれ方など) で調べることは有限群論の重要な問題である．(ii) についてはそれほど多くのことは知られていないが，(i) については前世紀末から今日まで多くの有用な結果が残されており，とくに近年 (1960 年以降) になって飛躍的進歩がなされた．後の §7.3 の目的は，(i) についての古典的結果から最近にいたるまでの結果の一部を解説することである．

b) 群の群への作用と半直積

G, V を (必ずしも有限ではない) 群とする．直積集合 $V\times G$ から V への写像

$$(v, g) \longmapsto v^g \qquad (v \in V,\ g \in G)$$

が与えられていて

(i)　$(uv)^g = u^g v^g$　$(u, v \in V,\ g \in G)$,

(ii)　$v^{gh} = (v^g)^h$　$(v \in V,\ g, h \in G)$,

(iii)　$v^1 = v$　($v \in V$, 1 は G の単位元)

が成り立つとき，G は V に**作用する**という．(i)は第4章の意味で V が作用域 G をもつ群であることを示す．また(ii), (iii)は第2章の意味で群 G が集合 V に作用していることを示す．したがって第2, 4章で定義された言葉を自由に用いるが，その主なものをここで復習しておこう：

(α)　V の部分集合 U と $G \ni g$ に対して

$$U^g = \{u^g \mid u \in U\}$$

とおく．G の任意の元 g に対して $U^g \subseteq U$ (実は等号となる)なるとき，U は G **不変**であるといわれる．また V の G 不変な部分群が自明なものに限るとき，G は V に**既約に作用**するという．

(β)　$C_G(V) = \{g \in G \mid v^g = v\ (\forall v \in V)\}$

は G の正規部分群である．これは G の V への作用の核にほかならない．$C_G(V) = 1$ のとき，G は V に**忠実に作用する**という．

(γ)　V の自己準同型 α: $v \mapsto v^\alpha$ が

$$(v^\alpha)^g = (v^g)^\alpha \qquad (\forall g \in G,\ \forall v \in V)$$

を満たすとき，α を G **自己準同型**という．V の G 自己準同型全体の集合を $\mathrm{End}_G(V)$ と書く．$\mathrm{End}_G(V)$ は単位元をもった半群である．V が Abel 群ならば $\mathrm{End}_G(V)$ は自然に環の構造をもつ．なお V の自己準同型全体の集合を $\mathrm{End}(V)$ で表わす．また V の自己同型，G 自己同型全体の集合をそれぞれ $\mathrm{Aut}(V)$, $\mathrm{Aut}_G(V)$ で表わす．

(δ)　$[V, G] = \langle v^{-1}v^g \mid v \in V,\ g \in G\rangle$,

$C_V(G) = \{v \in V \mid v^g = v\ (\forall g \in G)\}$

とおく．これらは V の G 不変な部分群で，$[V, G]$ は V の正規部分群である．——

一般に G が V に作用しているとき

(7.1)　G の V への作用の仕方から，G, V の構造について何がいえるか

ということを調べることが大切である．たとえば典型的な問題としては，

(7.2) $C_V(G)=1$, $(|V|, |G|)=1$ のとき V は可解であるか

があるが，これは現在未解決の問題である．しかし(7.2)の特別の場合として

(7.3) $C_V(G)=1$, $|G|=$素数ならば V は巾零である

という命題は真であり，それが本章のはじめで述べた Thompson の定理7.16である．このほかにも(7.1)に関する命題が後に取り扱われるであろう．

さて，つぎにあげるいくつかのよく知られた補題は，§7.2-§7.3の議論の基礎をなすものである．

補題 7.4(Schur) G が Abel 群 V に既約に作用しているとき，$\mathrm{End}_G(V)$ は斜体である．

証明 $\mathrm{End}_G(V)\ni\alpha\neq 0$ としよう．V^α は V の G 不変な部分群だから，既約性により $V^\alpha=V$ または $V^\alpha=1$ である．$\alpha\neq 0$ だから $V^\alpha=V$ である．一方，α の核 $\mathrm{Ker}\,\alpha$ も V の G 不変な部分群だから $\mathrm{Ker}\,\alpha=V$ または 1. $\alpha\neq 0$ により $\mathrm{Ker}\,\alpha=1$ である．したがって α は全単射となる．すなわち $\mathrm{End}_G(V)\ni\alpha\neq 0$ ならば，α は逆元をもち，したがって $\mathrm{End}_G(V)$ は斜体となる．▌

補題 7.5 有限 Abel 群 G が Abel 群 V に忠実かつ既約に作用しているとき，G は巡回群である．

証明 G は Abel 群で V に忠実に作用しているから自然に $G\subseteq\mathrm{End}_G(V)$ と考えることができる．また Schur の補題7.4により $\mathrm{End}_G(V)$ は斜体であるから，G は G によって生成される $\mathrm{End}_G(V)$ の可換部分体の乗法群の部分群である．したがって定理1.10により G は巡回群でなければならない．▌

問 7.3 有限群 G が Abel 群 V に忠実かつ既約に作用しているとき，G の中心 $Z(G)$ は巡回群であることを示せ．

補題 7.6 群 G が Abel 群 V に作用しているとする．$\mathrm{End}_G(V)\ni\varepsilon$, $\varepsilon^2=\varepsilon$ ならば，$V=V^\varepsilon\otimes V^{1-\varepsilon}$ である．

証明 $V\ni v$ ならば $v=v^\varepsilon\cdot v^{1-\varepsilon}$. よって $V=V^\varepsilon\cdot V^{1-\varepsilon}$. $V^\varepsilon\cap V^{1-\varepsilon}\ni v^\varepsilon=u^{1-\varepsilon}$ とすると，$v^\varepsilon=v^{\varepsilon^2}=u^{\varepsilon-\varepsilon^2}=u^{\varepsilon-\varepsilon}=u^0=1$. よって $V^\varepsilon\cap V^{1-\varepsilon}=1$. ▌

補題 7.7 G が Abel 群 V に作用していて，$|G|1_V\in\mathrm{Aut}_G(V)$ とする．このときつぎの(i), (ii)が成り立つ：

(i) $V=[V,G]\otimes C_V(G)$,

(ii) $V=V_0\otimes V_0'$, $V_0=G$ 不変ならば，V の或る G 不変部分群 V_1 が存在し

て $V=V_0\otimes V_1$.

証明 $|G|1_V\colon v\mapsto v^{|G|}\,(v\in V)$ は仮定により V の自己同型であるから，その逆写像を $v\mapsto v^{1/|G|}$ と書く.

$\varepsilon=\dfrac{1}{|G|}\sum_{g\in G}g\in \mathrm{End}(V)$ とおくと,

$$\varepsilon\in \mathrm{End}_G(V),\qquad \varepsilon^2=\varepsilon$$

である. 実際, $G\ni g$ のとき

$$g\varepsilon=\frac{1}{|G|}\sum_{g'}gg'=\Bigl(\frac{1}{|G|}\sum_{g'}gg'g^{-1}\Bigr)g=\varepsilon g,$$

$$\varepsilon^2=\frac{1}{|G|^2}\sum_{g,g'}gg'=\frac{1}{|G|^2}\sum_{g}\sum_{g'}gg'=\frac{1}{|G|^2}\sum_{g}|G|\varepsilon=\frac{1}{|G|^2}|G|^2\varepsilon=\varepsilon.$$

したがって補題7.6により $V=V^{\varepsilon}\otimes V^{1-\varepsilon}$. ところで $[V,G]=V^{1-\varepsilon}$, $C_V(G)=V^{\varepsilon}$ が容易にわかるから $V=[V,G]\otimes C_V(G)$ を得る.

(ii) $V=V_0\otimes V_0'$ の V_0 への射影を ρ とする. $\varepsilon=\dfrac{1}{|G|}\sum_{g}g\rho g^{-1}\in \mathrm{End}(V)$ とおく. 容易にわかるように

$$\varepsilon\in \mathrm{End}_G(V),\qquad V^{\varepsilon}\subseteqq V_0,\qquad v^{\varepsilon}=v\quad(\forall v\in V_0)$$

である. 後の二つから $\varepsilon^2=\varepsilon$ を得るから, 補題7.6により $V=V^{\varepsilon}\otimes V^{1-\varepsilon}$. $V^{\varepsilon}=V_0$ だから, $V_1=V^{1-\varepsilon}$ とおけばよい. ▌

補題7.7において, $(|G|,|V|)=1$ ならば $|G|1_V\in \mathrm{Aut}_G(V)$ なる条件が満たされることに注意して欲しい. 後に応用されるのは殆どこの場合だけである. 補題7.7の(ii)のつぎの系は有名である.

例題 7.1 (Maschke の定理) G を有限群, V を体 k 上の有限次元線型空間とし, G が V に作用しているとする. ただし G の元 g は V の線型変換をひき起すものとする. G の位数と k の標数が互いに素ならば, V は完全可約すなわち既約な G 不変部分空間の直和である.

[証明] G の位数と k の標数が互いに素だから, $|G|1_V\in \mathrm{Aut}_G(V)$ なる仮定が満たされている. V の G 不変部分空間で最小次元のものを V_0 とすると, V は線型空間だから $V=V_0\oplus V_0'$ なる V_0' が存在する. 補題7.7の(ii)を適用して V_0' も G 不変と仮定してよい. V_0' は既約な G 不変部分空間の直和と仮定してよいから(次元に関する帰納法), V もそうでなければならない. ▌

例題 7.2 有限群 G が有限 Abel 群 V に作用しているとする. さらに $(|G|,$

$|V|)=1$ と仮定する．V の素数位数の任意の元が G によって固定されるならば，G は V の各元を固定する．

［証明］ 補題7.7の(i)が適用できて $V=[V,G]\otimes C_V(G)$．$[V,G]=1$ をいえばよい．$[V,G]\neq 1$ として x を $[V,G]$ の素数位数の元とする．仮定により $x\in C_V(G)$ である．したがって $x\in[V,G]\cap C_V(G)$ となり矛盾である．▌

問 7.4 有限群 G が Abel 群 V に作用しているとする．$P\in \mathrm{Syl}_p(G)$，$[G:P]1_V\in \mathrm{Aut}_G(V)$ と仮定する．$V=V_0\otimes V_0'$，$V_0=G$ 不変，$V_0'=P$ 不変ならば，V の或る G 不変部分群 V_1 が存在して $V=V_0\otimes V_1$．［ヒント］ g_i を G/P の任意の代表系，ρ を $V=V_0\otimes V_0'$ から V_0 への射影とするとき，$\varepsilon=\dfrac{1}{[G:P]}\sum_i g_i\rho g_i^{-1}$ とおけ．——

さて，G が V に作用しているとき，G と V の半直積なる有用な概念を導入しよう．直積集合 $G\times V$ の上につぎのような(直積の群とは異なる)演算を定義する：

$$(g,v)(g',v')=(gg',v^{g'}v') \qquad (g,g'\in G,\ v,v'\in V).$$

このとき $G\times V$ はこの演算に関して群となることは見易い．

問 7.5 これを確かめよ．——

このようにして構成された群を G と V の**半直積**といい，それをしばらくのあいだ $G*V$ で表わす．半直積 $G*V$ の部分集合

$$\{(g,1)\mid g\in G\}, \qquad \{(1,v)\mid v\in V\}$$

は，それぞれ自然な対応 $g\mapsto(g,1)$，$v\mapsto(1,v)$ によって G,V と同型な $G*V$ の部分群である．よってこれらの部分群をこの対応によって G,V と同一視して，G,V を $G*V$ の部分群とみなすことにする．このとき

$$G*V=GV=VG\rhd V, \qquad V\cap G=1,$$
$$v^g=g^{-1}vg \qquad (v\in V,\ g\in G)$$

である．したがって半直積 $G*V$ を GV あるいは VG と書くことが多い．また上の(β)，(δ)で定義された $[V,G]$，$C_V(G)$，$C_G(V)$ などは，G,V を半直積 GV の部分群とみて，交換子や中心化群を作ったものにほかならない．また以後本書でしばしば用いられる $[V,G,G]$，$[G,V,V]$，… などの記号も上と同じように GV の部分群 G,V に対して(高階の)交換子を作る意味である．——

X を群，V を X の正規部分群としよう：$X\rhd V$.

$$X=GV, \qquad G\cap V=1$$

なる X の部分群 G が存在するとき，剰余群 X/V は**分裂する**といい，G を X/V の**補群**という．G が V に作用しているとき，その半直積 GV を X とすれば，X/V は分裂し，G がその補群である．逆に $X\triangleright V$，X/V が分裂するとき，その補群を G とすれば，G は V に自然に作用し G と V の半直積は X と同型である．

さて，X の正規部分群 V が与えられたとき，

(7.4) X/V が分裂するための条件，

(7.5) X/V が分裂するとき，その補群達の間の関係，たとえば二つの補群は互いに共役であるか

を調べることが，(有限)群論では重要となる．§7.2 の主題は，$|V|$ と $|X/V|$ が互いに素のとき，(7.4), (7.5) に対して 'Sylow 型' の定理 (Schur-Zassenhaus の定理) が成り立つことを示し，それを応用して G が V に作用し，$(|G|,|V|)=1$ なるときの基本事項を解説することである．

問 7.6 $\mathfrak{S}_n/\mathfrak{A}_n$ は分裂する．しかし $n\geqq 6$ のとき共役でない補群が存在する．

問 7.7 $\mathfrak{S}_4\triangleright V_4=\{(1),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$ に対して $\mathfrak{S}_4/V_4$ は分裂する．また $\mathfrak{S}_4/V_4$ の任意の二つの補群は互いに共役であることを示せ．

§7.2 Schur-Zassenhaus の定理とその応用

a) コホモロジー

有限群 G が Abel 群 A (A は無限群でもよい) に作用しているとする．G から A への写像 f が

(7.6) $$f(\sigma)^{\tau}f(\tau)=f(\sigma\tau) \qquad (\forall\sigma,\tau\in G)$$

なる等式を満たすとき，このような f を (G,A) の **1 双対輪体**という．$A\ni a$ に対して

(7.7) $$f(\sigma)=a^{1-\sigma} \qquad (\sigma\in G)$$

によって f を定義すると，これは 1 双対輪体である．このような 1 双対輪体は，**1 双対境界輪体**とよばれる．$G\times G$ から A への写像 f が

(7.8) $$f(\sigma,\tau)^{\rho}f(\sigma\tau,\rho)=f(\sigma,\tau\rho)f(\tau,\rho) \qquad (\forall\sigma,\tau,\rho\in G)$$

なる等式を満たすとき，このような f を **2 双対輪体**という．g を G から A への

任意の写像とするとき

$$(7.9)\qquad f(\sigma,\tau)=g(\sigma)^{\tau}g(\tau)g(\sigma\tau)^{-1}$$

とおくと，これは 2 双対輪体である．このような 2 双対輪体は **2 双対境界輪体**とよばれる．

補題 7.8 G と A の位数は互いに素とするとき，

(i) 任意の 1 双対輪体は 1 双対境界輪体である，

(ii) 任意の 2 双対輪体は 2 双対境界輪体である．

証明 f を (G,A) の 1 双対輪体とする．$c=\prod_{\sigma\in G}f(\sigma)$ とおいて (7.6) の両辺の σ についての積を作ると $\prod_{\sigma\in G}f(\sigma\tau)=c$ に注意して

$$(*)\qquad c^{\tau}f(\tau)^{|G|}=c$$

を得る．仮定により $|G|$ と $|A|$ は互いに素だから $|G|n\equiv1\ (\mathrm{mod}\,|A|)$ なる整数 n が存在する．上の $(*)$ の両辺を n 乗して $a=c^{n}$ とおくと，

$$a^{\tau}f(\tau)=a\quad すなわち\quad f(\tau)=a^{1-\tau}$$

となり，f は 1 双対境界輪体である．

(ii) f を 2 双対輪体とする．$h(\tau)=\prod_{\sigma\in G}f(\sigma,\tau)$ とおいて (7.8) の両辺の σ についての積を作ると

$$(**)\qquad h(\tau)^{\rho}h(\rho)=h(\tau\rho)f(\tau,\rho)^{|G|}$$

を得る．再び $|G|n\equiv1\ (\mathrm{mod}\,|A|)$ なる n をとり，$g(\tau)=h(\tau)^{n}$ とおくと $(**)$ の両辺を n 乗して

$$f(\tau,\rho)=g(\tau)^{\rho}g(\rho)g(\tau\rho)^{-1}\qquad(\forall\tau,\rho\in G)$$

となり，f は 2 双対境界輪体である．▌

(G,A) の n 双対輪体 $(n=1,2)$ の全体の集合 $Z^{n}(G,A)$ は，関数の積に関して自然に Abel 群の構造をもつ．このとき，n 双対境界輪体全体の集合 $B^{n}(G,A)$ は，$Z^{n}(G,A)$ の部分群である．その剰余群

$$H^{n}(G,A)=Z^{n}(G,A)/B^{n}(G,A)$$

を (G,A) の **n 次コホモロジー群**という．一般には $n>2$ に対しても n 次コホモロジー群が定義される．これらは，もともと位相幾何学において発生したものであるが，(上で定義した 1 次，2 次のコホモロジー群に限っても) 群論はもとより多元環論，整数論などに重要な応用がある．しかしここではこれらのことには全く立ち入らない．本書で必要なのは上の補題 7.8 だけである．

つぎの補題は，補題7.8の直接の応用であり，後に一般化される．

補題 7.9 $X \triangleright A$, A は Abel 群，$|A|$ と $|X/A|$ は互いに素とする．このときつぎが成り立つ：

(i) X/A は分裂する，

(ii) Y を X/A の補群，U を $|U|\,|\,|X/A|$ なる X の部分群とすれば，U の或る共役は Y に含まれる．とくに X/A の任意の二つの補群は互いに共役である．

証明 まず(i)を証明しよう．$G=X/A$ とおき，G の元を $\sigma, \tau, \rho, \cdots$ などで表わす：$G=\{\sigma, \tau, \rho, \cdots\}$．$G \ni \sigma = xA$ $(x \in X)$，$A \ni a$ に対して

$$a^\sigma = x^{-1}ax$$

とおけば，G は A に作用する．A は Abel 群だから，a^σ の定義は $\sigma=xA$ なる x のとり方によらないことに注意．$G \ni \sigma$ に対して $\sigma=u_\sigma A$ なる $u_\sigma \in X$ をとり，これを固定する．

$$u_{\sigma\tau}A = (u_\sigma A)(u_\tau A) = (u_\sigma u_\tau)A$$

より

$$u_\sigma u_\tau = u_{\sigma\tau} f(\sigma, \tau)$$

なる $f(\sigma, \tau) \in A$ が定まる．このとき，$f(\sigma, \tau)$ は2双対輪体である．実際，$(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$ の両辺を計算すると

$$(u_\sigma u_\tau)u_\rho = u_{\sigma\tau} f(\sigma, \tau) u_\rho = u_{\sigma\tau} u_\rho f(\sigma, \tau)^\rho = u_{\sigma\tau\rho} f(\sigma\tau, \rho) f(\sigma, \tau)^\rho,$$
$$u_\sigma(u_\tau u_\rho) = u_\sigma u_{\tau\rho} f(\tau, \rho) = u_{\sigma\tau\rho} f(\sigma, \tau\rho) f(\tau, \rho)$$

となり，これらを比べて

$$f(\sigma, \tau)^\rho f(\sigma\tau, \rho) = f(\sigma, \tau\rho) f(\tau, \rho)$$

を得る．補題7.8の(ii)を適用して

$$f(\sigma, \tau) = g(\sigma)^\tau g(\tau) g(\sigma\tau)^{-1}$$

なる G から A への写像 g が存在する．このとき $v_\sigma = u_\sigma g(\sigma)^{-1}$ とおくと，$Y=\{v_\sigma \mid \sigma \in G\}$ は X の部分群である．実際，

$$\begin{aligned}
v_\sigma v_\tau &= (u_\sigma g(\sigma)^{-1})(u_\tau g(\tau)^{-1}) \\
&= u_\sigma u_\tau g(\sigma)^{-\tau} g(\tau)^{-1} \\
&= u_{\sigma\tau} f(\sigma, \tau) g(\sigma)^{-\tau} g(\tau)^{-1} \\
&= u_{\sigma\tau} g(\sigma\tau)^{-1} \\
&= v_{\sigma\tau}
\end{aligned}$$

であるから，Y は X の部分群となる．また $X=\sum_{\sigma\in A}u_\sigma A=\sum_{\sigma\in A}v_\sigma A=YA$, $Y\cap A=1$ だから Y は X/A の補群である．

(ii) Y_1, Y_2 を X/A の補群とする．$Y_1=\{u_\sigma\mid\sigma\in G\}$, $Y_2=\{v_\sigma\mid\sigma\in G\}$ とすると，$u_\sigma u_\tau=u_{\sigma\tau}$, $v_\sigma v_\tau=v_{\sigma\tau}$ である．さらに $u_\sigma=v_\sigma f(\sigma)$ なる $f(\sigma)\in A$ が存在するが，$f(\sigma)$ は (G, A) の 1 双対輪体である．実際，

$$\begin{aligned} v_{\sigma\tau}f(\sigma\tau) = u_{\sigma\tau} = u_\sigma u_\tau &= (v_\sigma f(\sigma))(v_\tau f(\tau)) \\ &= v_\sigma v_\tau f(\sigma)^\tau f(\tau) \\ &= v_{\sigma\tau} f(\sigma)^\tau f(\tau) \end{aligned}$$

であるから，両辺を比べて

$$f(\sigma\tau) = f(\sigma)^\tau f(\tau)$$

を得る．補題 7.8 の (i) により $f(\sigma)=a^{1-\sigma}$ なる $a\in A$ が存在するが，このとき

$$a^{-1}u_\sigma a = u_\sigma a^{-\sigma}a = u_\sigma f(\sigma) = v_\sigma$$

となるから，$a^{-1}Y_1a=Y_2$ を得る．すなわち X/A の任意の二つの補群は互いに共役であることがわかった．最後に Y を X/A の補群，U を $|U|\,|\,|X/A|$ なる X の部分群としよう．$X_1=UA$ とおくと

$$UA = X_1 = X_1\cap X = X_1\cap YA = (X_1\cap Y)A, \qquad U\cap A = 1$$

であるから，U と $X_1\cap Y$ はともに X_1/A の補群である．よって既に証明されたことにより，$X_1\ni x$ が存在して

$$U^x = X_1\cap Y \quad \text{とくに} \quad U^x \subseteqq Y$$

を得る．▌

b) Schur-Zassenhaus の定理

補題 7.9 を一般化しよう．それは有限群論の基本定理の一つである．

定理 7.1 (Schur-Zassenhaus) $G\triangleright N$, $|N|$ と $|G/N|$ は互いに素とする．このとき

(i) G/N は分裂する．

さらに N または G/N が可解群ならば

(ii) H を G/N の補群，K を $|K|\,|\,|H|$ なる G の部分群とすれば，K の或る共役は H に含まれる．とくに G/N の二つの補群は互いに共役である．——

証明を始める前に二つの注意をしておこう．その一つはこの定理に直接関係したものであり，他の一つはこの定理の証明の方法に関する一般的注意である．

注意 1　有名な Feit–Thompson の定理"奇数位数の群は可解である"を用いれば，定理の (ii) の仮定'N または G/N の可解性'は不要である．なぜなら，$|N|$ と $|G/N|$ が互いに素のとき，N または G/N が奇数位数となり，Feit–Thompson の定理により N または G/N が可解となるからである．しかしながら，Schur–Zassenhaus の定理を用いずに Feit–Thompson の定理を証明することは期待し得ないことであるから，有限群論の初等的部分で Feit–Thompson の定理を用いるのは適当ではない．したがってその意味で，'N または G/N の可解性'の仮定は上の定理において必要である．

注意 2　有限群論では，或る命題 P を証明するとき，しばしば背理法がつぎのように用いられる．すなわち P が成立しないとして矛盾をだすわけであるが，P の仮定を満たし結論が成立しない最小位数の群 G(このような G を P に対する**最小位数の反例**という)をとり，G の性質を調べて矛盾を出すのである．G が P に対する最小位数の反例ならば，P の仮定を満たす G より位数の小さい群に対しては P の結論が成立するのであるから，上のような推論は群の位数に関する数学的帰納法(と背理法の組合せ)であるともいえる．人間は背理法をできれば避けたいという習性を持っているようである．しかし有限群論の多くの重要な命題(本書では後に証明する Thompson の定理 7.16 など)が，最小位数の反例を調べて矛盾を出すという推論によって証明されるから，あまり背理法を避けようとするのは得策ではない．

定理 7.1 の証明　まず (i) を示そう．G を (i) に対する最小位数の反例とする．p を $|N|$ を割る一つの素数，$P\in \mathrm{Syl}_p(N)$ とする．このとき補題 7.1 により

$$G=N_G(P)N \tag{7.10}$$

である．以下 G の性質を段階に分けて調べよう．

(α)　$G=N_G(P)$ である．

$G\neq N_G(P)$ ならば，$N_G(P)\triangleright N_G(P)\cap N$ で $N_G(P)\cap N$ の位数と指数は互いに素であるから，$N_G(P)/N_G(P)\cap N$ は補群 H をもつ．すなわち

$$N_G(P)=H\cdot(N_G(P)\cap N),\qquad H\cap N_G(P)\cap N=H\cap N=1.$$

このとき，(7.10) を用いて

$$G=HN,\qquad H\cap N=1$$

となり矛盾である．

(β)　$N=P$.

$N\neq P$ とする．G/P, N/P は定理の仮定を満たすから，$(G/P)/(N/P)$ は補群 L/P をもつ．このとき

$$G=LN,\qquad L\cap N=P \tag{7.11}$$

である．$N\neq P$ と仮定しているから，$G\neq L$ である．L, P も定理の仮定を満たす

から L/P は補群 H をもち，

$$L = HP, \qquad H \cap P = 1$$

となる．このとき (7.11) により

$$G = HN, \qquad H \cap N = H \cap L \cap N = H \cap P = 1$$

となり矛盾である．

(γ) P は Abel 群である．

P を非 Abel 群とする．P の交換子群を P' とすると $1 \neq P' \lhd G$. G/P', P/P' は定理の仮定を満たすから，$(G/P')/(P/P')$ は補群 L/P' をもち，

$$G = LP, \qquad L \cap P = P' \tag{7.12}$$

となる．また L, P' も定理の仮定を満たし，$P' \neq P$ より $L \neq G$ であるから，L/P' は補群 H をもつ：

$$L = HP', \qquad H \cap P' = 1.$$

(7.12) により

$$G = HP, \qquad H \cap P = H \cap L \cap P = H \cap P' = 1$$

となり矛盾となる．

(β), (γ) により G, P は補題 7.9 の仮定を満たす．したがって G/P は分裂することになり，G が (i) に対する反例であることに矛盾する．

つぎに (ii) を示そう．G を (ii) に対する最小位数の反例とする．H を G/N の補群，K を $|K| \mid |H|$ なる G の部分群で K のどの共役も H に含まれないとしよう．

(δ) K は G/N の補群である．

$G_1 = KN$ とおくと，

$$KN = G_1 = G \cap G_1 = G_1 \cap HN = (G_1 \cap H)N$$

であるから，K と $G_1 \cap H$ は G_1/N の補群である．K が G/N の補群でなければ $G \neq G_1$ すなわち $|G_1| < |G|$ であるから，G_1 に対して (ii) が成り立つ：

$$K^x = G_1 \cap H \qquad (\exists x \in G_1).$$

とくに $K^x \subseteq H$ となり矛盾である．

(ε) G/N が可解である．

G/N が非可解ならば，定理の仮定により N が可解である．N に含まれる G の極小正規部分群を P とすると，P は Abel 群であるから補題 7.9 の (ii) により

$P \neq N$ である．$G/P, N/P$ は定理の仮定を満たすから，$\bar{K}^{\bar{x}} \subseteqq \bar{H}$ なる $\bar{x} = xP \in G/P$ が存在する．このとき $K^x \subseteqq HP$ である．$N \neq P$ より $G \neq HP$ であるから，HP, P, K^x に対して(ii)は成り立つ．すなわち $K^{xy} \subseteqq H$ なる $y \in HP$ が存在することになり矛盾である．

(ε)により G/N は可解であるから，G/N の極小正規部分群を R/N とすると，R/N は p 群である．$G=R$ とすると，K, H はともに G の S_p 部分群となるから，Sylow の定理により K と H は共役となり矛盾である．したがって $G \neq R$ である．また明らかに

$$R = N(R \cap H) = N(R \cap K), \qquad R \cap H,\ R \cap K \in \mathrm{Syl}_p(R)$$

であるから，K を適当な共役におきかえて $R \cap H = R \cap K$ と仮定してよい．$P = R \cap H = R \cap K$ とおくと，$G \triangleright R$ に補題7.1の(ii)を適用して

$$G = N_G(P)N$$

である．また $G \triangleright R$ より $N_G(P) \supseteqq H, K$ である．$G \neq N_G(P)$ ならば，$N_G(P) \triangleright N_G(P) \cap N$ に対して(ii)が成り立つから，H, K は $N_G(P)$ で共役となり矛盾である．$G = N_G(P)$ すなわち $G \triangleright P$ ならば，$G/P \triangleright N/P$ に対して(ii)が成り立つから，$\bar{G} \ni \bar{x}$ が存在して $\bar{K}^{\bar{x}} = \bar{H}$ すなわち $K^x \subseteqq HP = H$ となり，やはり矛盾である．▌

ここで一つの約束をしておこう．

$G \triangleright N$, $\bar{G} = G/N$ とするとき，G の部分集合 X に対して，$\bar{X}$ によって G から $\bar{G}$ への自然準同型による X の像を表わす：

$$\bar{X} = \{xN \mid x \in X\}.$$

今後一区切りの推論の中で，どのような剰余群を考えているかが，前後の関係で明瞭なとき，このような記法をいちいち断わらずに用いることにする．

補題 7.10 N, Q は G の部分群で，つぎの条件(i), (ii), (iii)を満たすとする：

(i) $G \triangleright N$,

(ii) $(|Q|, |N|) = 1$,

(iii) Q または N は可解．

$\bar{G} = G/N$ のとき，

$$N_{\bar{G}}(\bar{Q}) = \overline{N_G(Q)}, \qquad C_{\bar{G}}(\bar{Q}) = \overline{C_G(Q)}$$

である．

証明 $\overline{N_G(Q)} \subseteq N_{\bar{G}}(\bar{Q})$, $\overline{C_G(Q)} \subseteq C_{\bar{G}}(\bar{Q})$ は明らかである. $N_{\bar{G}}(\bar{Q}) \ni \bar{x}$ としよう. このとき, $Q^x \subseteq QN$ である. (ii), (iii) により QN/N に Schur-Zassenhaus の定理が適用できる. よって, 或る $y \in N$ が存在して

$$Q^{xy} = Q$$

である. $xy=z$ とおくと, $\bar{x}=\bar{z}$, $z \in N_G(Q)$ であるから, $N_{\bar{G}}(\bar{Q}) \subseteq \overline{N_G(Q)}$ が得られた. とくに $\bar{x} \in C_{\bar{G}}(\bar{Q})$ ならば,

$$[z, Q] = [xy, Q] \subseteq Q \cap N = 1.$$

よって, $z \in C_G(Q)$. したがって $\bar{x} \in C_{\bar{G}}(\bar{Q}) \subseteq \overline{C_G(Q)}$ である. ▌

c) 可解群に関する P. Hall の定理

本項では, 最初に Schur-Zassenhaus の定理の応用として有限可解群に対して 'Sylow 型' の定理 (定理 7.2) が成り立つことを示し, これと第8章で証明される Burnside の定理を用いて, 可解群の或る特徴づけに関する結果 (定理 7.3, 7.4) を証明しよう. これらは, P. Hall によって 1937 年に得られたものである.

定理 7.2 (P. Hall) G を可解群, $|G|=mn$, $(m,n)=1$ とする. このときつぎの (i), (ii) が成り立つ:

(i) G は位数 m の部分群をもつ,

(ii) H を G の位数 m の部分群, K を $|K|\,|\,m$ なる G の部分群とするとき, K の或る共役は H に含まれる. とくに G の二つの位数 m の部分群は互いに共役である.

証明 位数に関する数学的帰納法による. P を G の極小正規部分群とすれば, P は或る素数 p に対する p 群である. $\bar{G}=G/P$, $|P|=p^e$ とおく.

(α) $p\,|\,m$ の場合: 数学的帰納法により $\bar{G}$ は位数 m/p^e の部分群 $\bar{H}=H/P$ をもつ. このとき H は G の位数 m の部分群である. K を $|K|\,|\,m$ なる部分群とすれば, $\bar{K}=KP/P$ は $|\bar{K}|\,|\,m/p^e$ なる $\bar{G}$ の部分群である. よって数学的帰納法により $\bar{K}^{\bar{x}} \subseteq \bar{H}$ なる $\bar{x}=xP \in \bar{G}$ が存在する. このとき $K^x \subseteq HP=H$ となる.

(β) $p \nmid m$ の場合: 数学的帰納法により $\bar{G}$ は位数 m の部分群 $L/P=\bar{L}$ をもつ. このとき, $|P|$ と $|L/P|$ は互いに素であるから Schur-Zassenhaus の定理により L/P は分裂し, その補群 H は G の位数 m の部分群である. K を $|K|\,|\,m$ なる G の部分群とすると, $\bar{K}=KP/P$ は $|\bar{K}|\,|\,m$ なる $\bar{G}$ の部分群だから数学的帰納法により $\bar{K}^{\bar{x}} \subseteq \bar{L}$, したがって $K^x \subseteq L$ となる. L/P, K^x に Schur-Zassenhaus の

定理の (ii) を適用して，或る $y \in L$ に対して $K^{xy} \subseteqq H$ となる．▌

つぎに進むために一つの補題を準備しよう．

補題 7.11　G を有限群，$H_1, H_2, \cdots, H_r$ は G の部分群で $[G:H_1], [G:H_2], \cdots$ $[G:H_r]$ のどの二つも互いに素とする．このとき，$[G:H_1 \cap H_2 \cap \cdots \cap H_r] = [G:H_1][G:H_2]\cdots[G:H_r]$ である．

証明　$r=2$ のときを証明すればよい．$[G:H_i]=m_i$，$[H_i:H_1 \cap H_2]=h_i$ $(i=1,2)$，$|H_1 \cap H_2|=a$ とおく．このとき，

$$|G| = h_1 m_1 a = h_2 m_2 a \quad とくに \quad h_1 m_1 = h_2 m_2$$

である．m_1 と m_2 は互いに素であるから，$h_2=m_1 s$, $h_1=m_2 s$ なる整数 s が存在し，

$$|G| = am_1m_2s$$

となる．一方

$$am_1m_2s = |G| \geqq |H_1H_2| = |H_1||H_2|/|H_1 \cap H_2| = \frac{m_1sam_2sa}{a} = am_1m_2s^2$$

であるから，$s=1$ かつ上の不等号は等号になる．すなわち $G=H_1H_2$．したがって

$$[G:H_1 \cap H_2] = |H_1H_2|/|H_1 \cap H_2| = |H_1||H_2|/|H_1 \cap H_2|^2 = m_1m_2$$

となる．▌

定理 7.3 (P. Hall)　G を可解群，$p_1, p_2, \cdots, p_r$ を $|G|$ を割るすべての素数とする．このとき，各 p_j に対して S_{p_j} 部分群 P_j を適当にとれば $P_iP_j=P_jP_i$ $(1 \leqq i \neq j \leqq r)$ となる．

証明　$|G|=p_1{}^{e_1}p_2{}^{e_2}\cdots p_r{}^{e_r}$ を $|G|$ の素因子分解とする．定理 7.2 により，G は位数 $|G|/p_i{}^{e_i}$ の部分群 H_i をもつ．

$$\bigcap_{k \neq i} H_k = P_i, \quad \bigcap_{k \neq i,j} H_k = H_{ij}$$

とおくと，$H_{ij} \supseteqq P_i, P_j$ である．また補題 7.11 により，$|P_i|=p_i{}^{e_i}$，$|H_{ij}|=p_i{}^{e_i}p_j{}^{e_j}$ となるから，$H_{ij}=P_iP_j=P_jP_i$ を得る．▌

つぎの定理は定理 7.3 の逆である．

定理 7.4　$|G|$ を割る各素数 p_i $(1 \leqq i \leqq r)$ に対して S_{p_i} 部分群 P_i を適当にとり，$P_iP_j=P_jP_i$ $(i \neq j)$ となるならば，G は可解群である．——

この定理の証明には，その特別の場合 $(r=2)$ であるつぎの Burnside の定理を使わねばならない．

W. Burnside の定理 G の位数がちょうど二つの素数で割れるとき G は可解群である．——

この Burnside の定理の証明は，本書では群指標の応用として第8章で述べる．近年になって Bender, Goldschmidt, 松山により群指標を用いない証明が得られ，それも非常に興味深いものであるが，それを述べるには少し準備が必要なのでここでは割愛せざるを得ない．

定理 7.4 の証明 $|G|=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, $K=P_1P_2$ とおく．Burnside の定理により $G\neq K$ としてよい．最初に G が単純群でないことを示そう．再び Burnside の定理により K は可解群であるから，その極小正規部分群を Q とすれば，Q は p_1 群か p_2 群である．一般性を失わずに Q は p_2 群であるとしてよい．定理の仮定により G は位数 $|G|/p_1^{e_1}$ の部分群(たとえば $P_2P_3\cdots P_r$)をもつ．H をそのような任意の部分群とすれば，$[G:H]=p_1^{e_1}$, $[G:K]=p_3^{e_3}\cdots p_r^{e_r}$ であるから，補題 7.11 により $H\cap K$ は G の S_{p_2} 部分群である．$K\triangleright Q$ であるから補題 7.1 の (i) により $Q\subseteqq H\cap K$ とくに $Q\subseteqq H$ である．H は位数 $|G|/p_1^{e_1}$ の任意の部分群であったから，

$$N=\bigcap_{x\in G}H^x \supseteqq Q \neq 1 \qquad (H^x=x^{-1}Hx)$$

となり，明らかに N は G の自明でない正規部分群である．ところで定理の仮定は N および G/N に対しても成り立つ．実際，$Q_i=P_i\cap N$, $\bar{P}_i=P_iN/N$ がそれぞれ N, G/N の S_{p_i} 部分群で定理の仮定を満たすことは容易に確かめられる．したがって位数に関する数学的帰納法により N および G/N は可解群となり，このとき G も可解群でなければならない．▌

問 7.8 G を有限群とする．$|G|=mn$, $(m,n)=1$ なる任意の m に対して位数 m の部分群が存在すれば，G は可解群であることを示せ(定理 7.2 の逆!)．——

本項の最初にもふれたように，定理 7.2, 7.3, 7.4 は P. Hall により 1937 年に証明されたものである．しかしこれらの定理が有限群論で有効に応用されだしたのは，1960 年代に入ってからである．前項 b) の注意 1 で引用した Feit-Thompson の定理の証明の中で，Thompson がこれを応用して以来，これらの定理は

有限群論で重要な役割を果たすようになってきた．本書でその直接の応用を述べられないのは残念であるが，これらの定理の形の美しさだけからでも読者の興味をひき起せれば幸いである．

d）素な作用

本項では，群 G が群 V に作用し，$|G|$ と $|V|$ が互いに素であるときの基本事項を説明する．最初に，以下の記述を簡単にするため言葉を定義しよう．

G が V に**素に作用**するとは，

(α) $|G|$ と $|V|$ は互いに素である，

(β) G または V が可解群

なる条件を満たすことである．b) の注意1におけるのと同じ理由で (β) は (α) からの帰結であるが，本書のような段階では (β) を仮定しなければならない．また G が V に作用し，

$$V=C_V(G) \quad \text{すなわち} \quad [V,G]=1$$

であるとき，G は V に**自明に作用**するという．

定理 7.5 A が X に作用しているとする．Y は X の A 不変正規部分群で，A は Y に素に作用しているとする．このとき

$$C_X(A)Y/Y=C_{X/Y}(A).$$

すなわち，$\bar{X}=X/Y$ とすると，$C_{\bar{X}}(A)=\overline{C_X(A)}$ である．

証明 A と X の半直積を G としよう：$G=AX$．このとき，$G \triangleright Y$ である．補題 7.10 の G, N, Q として，それぞれ AX, Y, A をとれば，

$$\overline{C_{AX}(A)}=C_{\overline{AX}}(\bar{A}).$$

$\overline{C_{AX}(A)}=Z(\bar{A})\cdot\overline{C_X(A)}$，$C_{\overline{AX}}(\bar{A})=Z(\bar{A})\cdot C_{\bar{X}}(\bar{A})=Z(\bar{A})\cdot C_{\bar{X}}(A)$ であるから，

$$Z(\bar{A})\cdot\overline{C_X(A)}=Z(\bar{A})\cdot C_{\bar{X}}(A)$$

を得る．$C_{\bar{X}}(A)\supseteqq\overline{C_X(A)}$ に注意すれば，$\overline{C_X(A)}=C_{\bar{X}}(A)$ を得る．▌

系 A が X に素に作用するとき，

(i) $X=[A,X]C_X(A)$,

(ii) $[X,A,A]=[X,A]$.

証明 $Y=[A,X]$ とおくと，補題 5.1 の (i) により Y は半直積 AX の正規部分群とくに A 不変である．$\bar{X}=X/Y$ とおく．このとき，$\bar{X}=C_{\bar{X}}(A)$ である．また

定理7.5により，$\overline{C_X(A)}=C_{\bar{X}}(A)$ であるから，$\bar{X}=\overline{C_X(A)}$ すなわち $X=C_X(A)Y$ を得る．これは(i)を示す．また，

$$[X, A]=[C_X(A)Y, A]=[Y, A]=[X, A, A].$$

すなわち(ii)が成り立つ．ここで第2の等号は(5.4)より出ることに注意．▌

問 7.9 A が X に素に作用しているとする．$X=YZ\triangleright Y$ で Y, Z は A 不変とするとき，$C_X(A)=C_Y(A)C_Z(A)$ であることを示せ．

補題 7.12 A が X に素に作用するとする．つぎの条件(i), (ii), (iii), (iv)の一つが成り立つとき，A は X に自明な作用をする：

(i) $[A, X]\subseteq\Phi(X)$．すなわち A が X の Frattini 剰余群 $X/\Phi(X)$ に自明な作用をする，

(ii) $X\triangleright Y$, $[A, X]\subseteq Y$, $[A, Y]=1$．すなわち A は $X/Y, Y$ に自明な作用をする，

(iii) $X\triangleright Y$, $C_X(Y)\subseteq Y$, $[A, Y]=1$,

(iv) X は巾零群，$X\supseteq Y$, $C_X(Y)\subseteq Y$, $[A, Y]=1$.

証明 (i) $[A, X]\subseteq\Phi(X)$ および定理7.5の系により，$X=C_X(A)\Phi(X)$．補題7.2を用いて，

$$X=C_X(A)\Phi(X)=\langle C_X(A), \Phi(X)\rangle=\langle C_X(A)\rangle=C_X(A)$$

を得る．(ii) $X=[X, A]C_X(A)=YC_X(A)=C_X(A)$．(iii) 半直積 AX を考えて，その部分群 A, Y, X に対して3部分群補題5.8を適用する．$[A, Y, X]=[1, X]=1$, $[Y, X, A]\subseteq[Y, A]=1$ ($X\triangleright Y$ より $[Y, X]\subseteq Y$ に注意)であるから，$[X, A, Y]=1$ である．よって $[X, A]\subseteq C_X(Y)\subseteq Y$．このとき，(ii)により $[X, A]=1$ である．(iv) X は巾零群だから，定理5.1により，

$$X=Y_n\triangleright Y_{n-1}\triangleright\cdots\triangleright Y_1\triangleright Y_0=Y$$

なる X の部分群の列 $Y_0, Y_1, \cdots, Y_n$ が作れる．容易にわかるように $C_X(Y_i)\subseteq Y_i$ ($i=0, 1, 2, \cdots, n$) である．このとき，(iii)を繰返し用いて $[A, Y_i]=1$ ($i=0, 1, 2, \cdots, n$) を得る．とくに $[A, X]=[A, Y_n]=1$ である．▌

この補題7.12は，以後しばしば用いられる大切な補題である．たとえば，補題7.12において X を有限可解群としよう．このとき

$$[A, F(X)]=1 \Longrightarrow [A, X]=1 \qquad (F(X) \text{ は } X \text{ の Fitting 部分群})$$

である．実際，$X\triangleright F(X)$，また定理5.6により $C_X(F(X))\subseteq F(X)$ であるから，

補題 7.12 の (iii) が適用できる．

つぎの定理は，Sylow の定理の精密化である，

定理 7.6 A が X に素に作用しているとする．p を $|X|$ を割る素数とするとき

(i) A 不変な X の S_p 部分群が存在する，

(ii) P を A 不変な X の S_p 部分群，Q を A 不変な X の p 部分群とすると，$Q^x \subseteq P$ なる $x \in C_X(A)$ が存在する．

証明 G を A と X の半直積とする：$G = AX \triangleright X$．$P \in \mathrm{Syl}_p(X)$ とすると補題 7.1 により

$$G = N_G(P)X, \qquad G/X \simeq N_G(P)/N_G(P) \cap X$$

である．よって $N_G(P)/N_G(P) \cap X$ に Schur-Zassenhaus の定理を適用して，その補群を A_1 とすれば，それは G/X の補群でもある．再び Schur-Zassenhaus の定理により $A^x = A_1$ なる $x \in X$ が存在する．このとき $A_1 \subseteq N_G(P)$ より P は A^x 不変したがって $P^{x^{-1}}$ は A 不変な X の S_p 部分群である．これで (i) が証明された．つぎに (ii) を示そう．Q を含む X の A 不変な p 部分群で極大なものを P_1 とする．$N_X(P_1)$ は A 不変だから，(i) により $N_X(P_1)$ の A 不変 S_p 部分群 $P_2 \supseteq P_1$ が存在する．$P_2 \neq P_1$ ならば $N_{P_2}(P_1) \supsetneqq P_1$ かつ $N_{P_2}(P_1)$ は A 不変だから P_1 の極大性に反する．よって $P_2 = P_1$ である．これは P_1 が X の S_p 部分群であることを示す．したがって (ii) を示すとき Q も A 不変 S_p 部分群としてよい．Sylow の定理により $P^x = Q$ なる $x \in X$ が存在する．このとき $N_G(Q) \supseteq A^x, A$ である．$N_G(Q)/N_G(Q) \cap X$ に Schur-Zassenhaus の定理を適用して，$A^{xy} = A$ なる $y \in N_G(Q) \cap X$ が存在する．このとき，$xy \in X$ に注意して

$$[xy, A] \subseteq A \cap X = 1 \quad \text{すなわち} \quad xy \in C_X(A),$$
$$P^{xy} = Q^y = Q$$

である．▌

系 A が X に素に作用しているとする．P を X の A 不変 S_p 部分群とするとき，A の任意の部分群 B に対して $C_P(B)$ は $C_X(B)$ の S_p 部分群である．

証明 $C_P(B)$ を含む $C_X(B)$ の B 不変 S_p 部分群を P_1，P_1 を含む X の B 不変 S_p 部分群を P_2 とすると，$C_{P_2}(B) = P_1$ である．また定理 7.6 により $P^x = P_2$ なる $x \in C_X(B)$ が存在する．$x \in C_X(B)$ であるから，$C_P(B)^x = C_{P^x}(B) = C_{P_2}(B)$

$=P_1$ となり，$C_P(B)$ は $C_X(B)$ の S_p 部分群である．▌

問 7.10　A が X に素に作用しているとき，つぎの (i), (ii) を示せ：

(i)　X の A 不変極小部分群は，或る素数に対する基本 Abel 群である，

(ii)　半直積 AX において，A が AX の極大部分群ならば，X は或る素数に対する基本 Abel 群である．

問 7.11　A が可解群 X に素に作用しているとする．$|X|=mn$，$(m, n)=1$ とする．このとき，つぎの (i), (ii), (iii) を示せ：

(i)　X の位数 m の A 不変部分群が存在する，

(ii)　Y を位数 m の A 不変部分群，Z を $|Z|\,|\,m$ なる任意の A 不変部分群とするとき，$C_X(A)$ の或る元 x が存在して，$Z^x \subseteq Y$ である，

(iii)　$|M|\,|\,m$ なる $AC_X(A)$ 不変な部分群 M で最大のものが存在する．

[ヒント]　定理 7.2 の応用．定理 7.6 の証明を参考にせよ．——

A を Abel 群とするとき，$m(A)$ によって A の生成元の最小個数，すなわち A を $A_1 \otimes A_2 \otimes \cdots \otimes A_r$，$|A_1|\,|\,|A_2|\,|\cdots|\,|A_r|$ なる巡回群 A_i の直積に分解したときの直積因子の個数を表わす：

$$m(A) = (A \text{ の生成元の最小個数}).$$

とくに $m(A)=1$ は，A が巡回群であることを示す．また，群 G に対して

$$G^\sharp = G - \{1\}$$

とおく．

定理 7.7　Abel 群 A が X に素に作用しているとき，

$$X = \langle C_X(A_0) \,|\, m(A/A_0)=1 \rangle$$

である．ここで，A_0 は $m(A/A_0)=1$ なる A のすべての部分群を走る．

証明　p を $|X|$ を割る素数，P を X の A 不変 S_p 部分群とする．このとき，

$$P = \langle C_P(A_0) \,|\, m(A/A_0)=1 \rangle$$

を示せば十分である．$\bar{P}=P/\Phi(P)$ ($\Phi(P)$ は P の Frattini 部分群) とおく．$\bar{P}$ は基本 Abel 群だから，標数 p の素体の上の線型空間と考えることができる．p は $|A|$ と素だから，Maschke の定理 (例題 7.1) を用いて，

$$\bar{P} = \bar{P}_1 \oplus \bar{P}_2 \oplus \cdots \oplus \bar{P}_r, \qquad \bar{P}_i \text{ は } A \text{ 既約}$$

となる．A の $\bar{P}_i$ への作用の核を A_i とすると，補題 7.5 により，A/A_i は巡回群すなわち $m(A/A_i)=1$ である．よって

$$\bar{P}=\langle C_{\bar{P}}(A_i)\,|\,1\leqq i\leqq r\rangle=\langle C_{\bar{P}}(A_0)\,|\,m(A/A_0)=1\rangle$$

を得る．ところで，定理7.5により，$C_{\bar{P}}(A_0)=\overline{C_P(A_0)}$ であるから，

$$\begin{aligned}P&=\langle C_P(A_0),\Phi(P)\,|\,m(A/A_0)=1\rangle\\&=\langle C_P(A_0)\,|\,m(A/A_0)=1\rangle\qquad(\text{補題}7.2)\end{aligned}$$

を得る．▮

定理7.7は，A が巡回群のときは自明であり，実質的効果をもつのは，A が巡回群でない場合である．A が非巡回群のとき，定理7.7をつぎの形で用いることが多い：

(7.13)　　$X=\langle C_X(a)\,|\,a\in A^{\sharp}\rangle\qquad(A^{\sharp}=A-\{1\})$.

これは，$m(A/A_0)=1$ なる A_0 に対して，$A_0^{\sharp}\ni a$ をとると明らかに $C_X(a)\supseteqq C_X(A_0)$ であるから，定理7.7の直接の結果である．(7.13)は，X が $A^{\sharp}$ の各元の固定点で生成されることを示している．このことから，$A^{\sharp}$ の各元の固定部分群達の性質と X の性質の関係に注目するのは自然である．つぎの例題は，そのような関係を示すもっとも簡単なものである．

例題7.3　Abel群 A が X に素に作用し，$A^{\sharp}$ の任意の元 a に対して $C_X(a)$ は巾零群であるとする．このとき，$m(A)\geqq 3$ ならば，X も巾零群である．

[証明]　$|X|$ を割る素数 p,q をとる．P,Q をそれぞれ X の A 不変 S_p 部分群，S_q 部分群とするとき，

$$[P,Q]=1$$

を示せば十分である．定理7.7により

(7.14)　　$P=\langle C_P(A_0)\,|\,m(A/A_0)=1\rangle$

である．$m(A/A_0)=1$ なる A_0 を一つ固定しよう．$m(A)\geqq 3$ により，A_0 は非巡回群であるから，A_0 の Q への作用に対して(7.13)を適用すれば，

(7.15)　　$Q=\langle C_Q(a)\,|\,a\in A_0^{\sharp}\rangle$

である．ところで，$C_P(A_0)$ と $C_Q(a)\,(a\in A_0^{\sharp})$ は，それぞれ巾零群 $C_X(a)$ の p 部分群と q 部分群であるから，

$$[C_P(A_0),C_Q(a)]=1$$

を得る．したがって(7.15)により

(7.16)　　$[C_P(A_0),Q]=1$

を得る．A_0 は $m(A/A_0)=1$ なる任意の部分群であるから，(7.14)，(7.16)から，

$$[P, Q] = 1$$

となる. ▌

例題 7.3 において $m(A)=2$ のときは, X は(必ずしも巾零群とは限らない)可解群であることが知られているが, その証明は少し面倒である. また例題 7.3 のつぎのような一般化も知られている:

(7.17) $m(A) \geqq 3$, $C_X(a) =$ 可解 $(\forall a \in A^\sharp) \Longrightarrow X =$ 可解.

しかし, この主張を含むより一般的かつ重要な結果がある. それがつぎに説明するいわゆる信号関手定理 (signalizer functor theorem) である.

今後, 素数 p に対して位数が p と素な群を **p' 群**ということにしよう.

G を任意の有限群, p を素数, A, X は G の部分群で

A は $m(A) \geqq 2$ なる可換 p 群,

X は G の A 不変 p' 部分群 $(N_G(X) \supseteqq A)$

とする. $A^\sharp \ni a$ に対して

$$\theta(C_G(a)) = C_X(a)$$

とおく. まず (7.13) により

$$X = \langle \theta(C_G(a)) \mid a \in A^\sharp \rangle$$

である. さらにつぎの (α), (β) が成り立つことは自明である:

(α) $\theta(C_G(a))$ は $C_G(a)$ の A 不変 p' 部分群,

(β) $\theta(C_G(a)) \cap C_G(b) \subseteq \theta(C_G(b))$ $(\forall a, b \in A^\sharp)$.

ここで, 逆につぎの問題を考える:

(7.18) 有限群 G の $m(A) \geqq 2$ なる可換 p 部分群 A と $A^\sharp$ の各元 a に対して, (α), (β) を満たす G の部分群 $\theta(C_G(a))$ が与えられたとき, G の A 不変 p' 部分群 X が存在して $\theta(C_G(a)) = C_X(a)$ $(\forall a \in A^\sharp)$ であるか. いいかえると, $X = \langle \theta(C_G(a)) \mid a \in A^\sharp \rangle$ とおくとき, X は A 不変 p' 部分群で $\theta(C_G(a)) = C_X(a)$ であるか. ——

この問題は, $m(A)=2$ のときは反例があって真ではない. また $m(A) \geqq 3$ のときも, 一般には未解決であるが, $\theta(C_G(a))$ が $A^\sharp$ の任意の元 a に対して可解群ならば, 上の問題 (7.18) は真であることが知られている. すなわちつぎの定理が成り立つ:

信号関手定理 (Glauberman-Goldschmidt-Gorenstein) $m(A) \geqq 3$ で $A^\sharp$ の

各元 a に対して $\theta(C_G(a))$ が可解群ならば，$X=\langle\theta(C_G(a))\,|\,a\in A^\sharp\rangle$ は**可解な** A 不変 p' 部分群で，$\theta(C_G(a))=C_X(a)$ である．

問 7.12　この定理が (7.17) の主張を含むことを確認せよ．——

この信号関手定理は，奇数位数の群の可解性に関する Feit-Thompson の定理の超難解な原証明の重要な一部に含まれていた原理を明確にしたものであり，さらに近年の有限単純群論においても大切な役割を果たしている．本書では，後の §7.4, d) において信号関手定理の $p=2$ の場合の Bender による証明を与えるであろう．p が奇素数のときも，$m(A)\geqq 4$ ならば，Goldschmidt による比較的簡単な(しかも p の偶奇にかかわらず通用する)証明が知られているが，本書では割愛する．なお，p が奇素数で $m(A)=3$ のときの証明 (Glauberman) は，現在のところかなり難解である．ここでは，差し当り言葉の定義と可移性定理の証明を述べておくことにする．

G を有限群，A を G の可換 p 部分群で $m(A)\geqq 2$ とする．$A^\sharp$ の各元 a に対して，上の (α), (β) を満たす G の部分群 $\theta(C_G(a))$ が与えられているとき，

$$a\longmapsto\theta(C_G(a))$$

なる対応 θ を，G の A **信号関手** (A-signalizer functor) という．なお，A 信号関手の典型的な例は，§7.4, a)で与えるであろう (例題 7.7 参照)．$A^\sharp$ の各元 a に対して $\theta(C_G(a))$ が可解群のとき，このような A 信号関手は**可解**であるという Feit-Thompson の定理によれば，$p=2$ のとき A 信号関手は常に可解である．また信号関手定理は，$m(A)\geqq 3$ のとき，可解な A 信号関手は，A 不変な可解 p' 部分群の別名にほかならないことを示している．

G の部分群 Y がつぎの条件 (γ), (δ) を満たすとき，Y を θ **部分群**という：

(γ)　Y は A 不変 p' 群,

(δ)　$C_Y(a)\subseteqq\theta(C_G(a))$　$(\forall a\in A^\sharp)$.

定義から，つぎのことは容易にわかる：

(7.19)　θ 部分群の A 不変部分群は θ 部分群である,

(7.20)　$\theta(C_G(a))$ は θ 部分群である (条件 (β) による).

G の θ 部分群全体の集合を $\mathit{U}_\theta(A)$，素数 q に対して $\mathit{U}_\theta(A)$ の元で q 群であるものを $\mathit{U}_\theta(A;q)$ と書く：

$$\mathit{U}_\theta(A;q)=\{Y\in\mathit{U}_\theta(A)\,|\,Y=q\ 群\}.$$

また，

$$\theta(C_G(A))=\bigcap_{a\in A^\sharp}\theta(C_G(a))$$

とおく．つぎのことも容易に確かめられる：

(7.21)　問題(7.18)の結論が成り立つためには，$И_\theta(A)$ がただ一つの極大元をもつことが必要十分である，

(7.22)　$\theta(C_G(A))\ni x$,　$И_\theta(A)\ni Y$　ならば　$Y^x=x^{-1}Yx\in И_\theta(A)$.

問 7.13　(7.19)-(7.22)を確かめよ．——

$И_\theta{}^*(A;q)$ によって $И_\theta(A;q)$ の極大元全体の集合を表わすとき，(7.22)により $\theta(C_G(A))$ は $И_\theta{}^*(A;q)$ の上に作用している．この作用についてつぎの重要な定理が成り立つ：

定理 7.8(可移性定理)　$m(A)\geqq 3$ のとき，$\theta(C_G(A))$ の $И_\theta{}^*(A;q)$ 上への作用は可移である．

注意　この定理では，'$\theta(C_G(a))$ の可解性' の仮定は必要でない．また，つぎのような認識は大切である．問題(7.18)の結論が成立することを想定するとき，すなわち

$$X=\langle\theta(C_G(a))\mid\forall a\in A^\sharp\rangle \text{ が } A \text{ 不変 } p' \text{ 部分群},$$
$$C_X(a)=\theta(C_G(a))\qquad(\forall a\in A^\sharp)$$

であることを想定するとき，

$$C_X(A)=\theta(C_G(A)),$$
$$И_\theta{}^*(A;q)\ni Q\Longrightarrow Q\in \mathrm{Syl}_q(X)$$

となり，可移性定理は定理7.6にほかならない．したがって，$m(A)\geqq 3$ のとき，問題(7.18)の結論が証明される前に，定理7.6に相当することがわかるところに可移性定理の意味があるのである．またこのことは，$m(A)\geqq 3$ ならば問題(7.18)が真であることを期待してもよいことを暗示しているということもできるであろう．

可移性定理の証明の前に，一つの簡単な補題を証明しよう．

補題 7.13　A は可換 p 群で，p' 群 X_1, X_2 に作用しているとする．$m(A)\geqq 3$ のとき，$C_{X_1}(a)\neq 1$，$C_{X_2}(a)\neq 1$ なる $A^\sharp$ の元 a が存在する．

証明　A は X_1, X_2 に既約に作用しているとしてよい．このとき，X_1, X_2 はそれぞれ基本 Abel 群である(問7.10)．A の $X_i\,(i=1,2)$ への作用の核を A_i とすると，補題7.5により A/A_i は巡回群である．したがって $m(A)\geqq 3$ により，$A_1\cap A_2\neq 1$．よって $A_1\cap A_2\ni a\neq 1$ をとると，$C_{X_1}(a)\neq 1$，$C_{X_2}(a)\neq 1$ である．▌

可移性定理の証明　$\theta(C_G(A))$ の $И_\theta{}^*(A;q)$ の上への作用の軌道が二つ以上あ

ると仮定して矛盾を導く．$И_\theta^*(A;q)\ni Q_1, Q_2$ を異なる軌道に属しかつ $|Q_1\cap Q_2|$ が最大になるようにとる．$H=Q_1\cap Q_2$, $R_i=N_{Q_i}(H)\,(i=1,2)$ とおく．$Q_1\neq Q_2$ であるから，$R_i\supsetneqq H$ である．A の $\bar{R}_i=R_i/H\ (i=1,2)$ への作用に対して，上の補題を適用すれば，$C_{\bar{R}_i}(a)\neq 1$ なる $a\in A^\sharp$ が存在する．このとき，定理7.5により $C_{R_i}(a)\subsetneqq H$ である．$N_0=N_G(H)\cap\theta(C_G(a))$ とおくと，(7.19), (7.20) により，$И_\theta(A)\ni N_0\supseteqq C_{R_i}(a)\ (i=1,2)$ である．また A の N_0 への作用を考えると，定理7.6により，$Q_0=\langle C_{R_1}(a)^x, C_{R_2}(a)\rangle$ が N_0 の A 不変 q 部分群であるような $x\in C_{N_0}(A)\subseteqq\theta(C_G(A))$ が存在する．$Q_0\in И_\theta(A)$ であるから，θ 部分群の定義と問7.9により，$Q_0H\in И_\theta(A)$ を得る．Q_0H は q 部分群だから，$Q_0H\subseteqq Q^*\in И_\theta^*(A;q)$ とすれば，$Q^*\cap Q_1^x\supseteqq C_{R_1}(a)^xH\supsetneqq H$, とくに $|Q^*\cap Q_1^x|>|Q_1\cap Q_2|$ となり，$|Q_1\cap Q_2|$ の極大性により Q^* と Q_1^x は同じ軌道に属する．よって，$x\in\theta(C_G(A))$ であったから，Q^* と Q_1 は同じ軌道に属する．同様に，$Q^*\cap Q_2\supseteqq C_{R_2}(a)H\supsetneqq H$ より，Q^* と Q_2 が同じ軌道に属する．このとき，Q_1 と Q_2 が同じ軌道に属することになり矛盾である．▮

問 7.14 $И_\theta^*(A;q)\ni Q$, B を A の部分群とするとき，$C_Q(B)$ は，$\theta(C_G(B))=\bigcap_{b\in B^\sharp}\theta(C_G(b))$ の S_q 部分群であることを示せ．［ヒント］定理7.8を用いて定理7.5の系の証明の真似をせよ．

例題 7.4 $A^\sharp$ の各元 a に対して $\theta(C_G(a))$ は巾零群とする．$m(A)\geqq 3$ のとき，$X=\langle\theta(C_G(a))\,|\,a\in A^\sharp\rangle$ は巾零な p' 部分群で $\theta(C_G(a))=C_X(a)\ (\forall a\in A^\sharp)$ である．すなわち $m(A)\geqq 3$ かつ $\theta(C_G(a))\ (\forall a\in A^\sharp)$ が巾零のときは，問題(7.18)は真である．

［証明］ $A^\sharp$ のすべての元 a を動かして $|\theta(C_G(a))|$ を割る素数全体の集合を π としよう．$\pi\ni q_1, q_2$ に対して，$И_\theta^*(A;q_i)\ni Q_i$ をとれば

$$[Q_1, Q_2]=1$$

であることが，例題7.3と全く同様にして証明される．このとき，

$$X_0=\langle Q\,|\,Q\in И_\theta^*(A;q),\ q\in\pi\rangle \tag{7.23}$$

は巾零群となり，問7.9により $X_0\in И_\theta(A)$ である．とくに $C_{X_0}(a)\subseteqq\theta(C_G(a))$ である．さて，$X_0=\langle\theta(C_G(a))\,|\,a\in A^\sharp\rangle$ を示せばよい．$И_\theta^*(A;q)\ni Q$ のとき，問7.14により $C_Q(a)$ は $\theta(C_G(a))$ の S_q 部分群であるから，(7.23) から，$\theta(C_G(a))\subseteqq X_0$, とくに $\theta(C_G(a))\subseteqq C_{X_0}(a)$ がわかる．よって $\theta(C_G(a))=C_{X_0}(a)$ である．このとき，

定理 7.7 により

$$X_0 = \langle C_{X_0}(a) \mid a \in A^\sharp \rangle = \langle \theta(C_G(a)) \mid a \in A^\sharp \rangle$$

を得る. ▌

e) Frobenius 群 I

有限群 G がつぎの性質をもつ自明でない正規部分群 N をもつとき, G を **Frobenius 群**という:

(7.24) $$N^\sharp \ni x \Longrightarrow C_G(x) \subseteq N \qquad (N^\sharp = N - \{1\}).$$

このような N を G の **Frobenius 核**という. 簡単のために, G が Frobenius 群で N がその Frobenius 核であるとき, (G, N) は Frobenius 群であるということにしよう. N が G に対して一意的に定まることは後にわかる (§7.3, e) 定理 7.17).

例 7.1 (i) 3 次対称群 $\mathfrak{S}_3$ は Frobenius 群である. 位数 3 の部分群が Frobenius 核である. もっと一般に, 位数 pq (p, q は素数, $p<q$) の非可換群は Frobenius 群で, 位数 q の部分群が Frobenius 核である.

(ii) 4 次交代群 $\mathfrak{A}_4$ は, $V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ を Frobenius 核とする Frobenius 群である.

(iii) F_q を q 個の元からなる有限体とするとき,

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \middle| a, b \in F_q,\ a \neq 0 \right\},$$

$$N = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \middle| b \in F_q \right\}$$

とおくと, (G, N) は Frobenius 群である.

(iv) $q-1 = 2^e r$ (r は 1 より大きい奇数) とする. α を有限体 F_q の乗法群の位数 r の元とするとき,

$$G = \left\{ \begin{bmatrix} \alpha^s & x & y \\ 0 & \alpha^{-s} & z \\ 0 & 0 & 1 \end{bmatrix} \middle| x, y, z \in F_q,\ s \in \boldsymbol{Z} \right\},$$

$$N = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \middle| x, y, z \in F_q \right\}$$

とおくと, (G, N) は Frobenius 群である.

補題 7.14　G を任意の有限群，H はその部分群で

$$H^{\sharp} \ni x \Longrightarrow C_G(x) \subseteq H \tag{7.25}$$

なる条件を満たすとき，H の位数と指数は互いに素である．

証明　$P \in \mathrm{Syl}_p(H)$，$P \subseteq P_0 \in \mathrm{Syl}_p(G)$ とするとき，$P=P_0$ をいえばよい．$Q = N_{P_0}(P)$ とおくと，$Q \triangleright P$ より $Z(Q) \cap P \neq 1$．$Z(Q) \cap P \ni x \neq 1$ とすると，(7.25) により $P \subseteq Q \subseteq C_G(x) \subseteq H$．よって $P \in \mathrm{Syl}_p(H)$ より $N_{P_0}(P)=P$ を得るが，これは $P=P_0$ を示す．▌

(G, N) が Frobenius 群のとき，(7.24) と補題 7.14 により $|G/N|$ と $|N|$ は互いに素である．したがって Schur-Zassenhaus の定理により

$$G = HN, \qquad H \cap N = 1$$

なる G の部分群 H が存在する．このような H を (G, N) の **Frobenius 補群**という．Frobenius 補群についてつぎの補題は大切である．

補題 7.15　H を Frobenius 群 (G, N) の Frobenius 補群とするとき，

$$G-H \ni x \Longrightarrow H \cap H^x = 1. \tag{7.26}$$

証明　$G \ni x=hn\,(h \in H,\ n \in N)$ とする．$H^x=H^n$ である．$H \cap H^n \neq 1$ ならば，$h=k^n$ なる H の元 h, k が存在する．このとき，$k^{-1}h=k^{-1}k^n=[k, n] \in N \cap H=1$．よって $k=h=k^n$．(7.24) により $n=1$．これは $x \in H$ を示す．▌

ここで Frobenius 群の定義について注意しておこう．つぎの条件は同値であることが知られている：

(i)　有限群 G は (7.24) を満たす真の正規部分群 N をもつ，

(ii)　有限群 G は (7.26) を満たす真の部分群 H をもつ．

すなわち，Frobenius 群の定義としては，(i), (ii) のどちらを採用してもよいのである．(i) $\Longrightarrow$ (ii) は補題 7.15 からわかる．しかし，(ii) $\Longrightarrow$ (i) を証明するためには，現在のところ群指標を用いる方法しか知られていない．したがって本講でもそれによって第8章で (ii) $\Longrightarrow$ (i) を証明するであろう．実は，Frobenius 群の定義としては，(ii) を採用する方が普通であるが，本講では都合上 (i) を定義として採用した．

(ii) は置換群論的につぎのような意味がある．(G, Ω) はつぎの条件を満たす置換群としよう：

(α)　G は Ω 上可移である，

(β) Ω 上の異なる 2 点を固定する G の元は単位元に限る,

(γ) G は Ω 上正則ではない.

このとき, Ω 上の任意の 1 点の固定部分群を H とすると, G, H は (7.26) を満たすことが容易にわかる. 逆に G, H が (7.26) を満たすとき, $\Omega=G/H$ とおくと G の Ω への作用は忠実で (α), (β), (γ) を満たす.

問 7.15 これらを確かめよ. ——

したがって, Frobenius 群を (α), (β), (γ) を満たす置換群として定義することもできるのである. このような Frobenius 群の観点も大切である. 一般に (G, Ω) が 2 重可移群で Ω の或る点 x (したがってすべての点) の固定部分群 G_x が, Frobenius 群 (すなわち, $(G_x, \Omega-\{x\})$ が (α), (β), (γ) を満たす置換群) のとき, (G, Ω) を **Zassenhaus 群**という.

例 7.2 (i) $PGL(2, q)$ や, $PSL(2, q)$ を 1 次元射影空間の上に例 2.3 のように作用させると, これらは Zassenhaus 群である.

(ii) $q=2^p$ (p は素数) とする.

$$F_q \ni x \longmapsto ax^{2^i}+b \qquad (a, b \in F_q,\ a \neq 0,\ 0 \leqq i \leqq p-1)$$

なる F_q 上の置換全体は, 可解な Zassenhaus 群である.

問 7.16 例 7.2 の (i), (ii) を確かめよ. ——

Zassenhaus 群の研究は, 1935 年の Zassenhaus の研究に始まり, 1950 年代に入ってから, Suzuki, Ito, Feit, Thompson らの努力により, 1960 年にその分類が完成された. その分類の過程で, Suzuki によるいわゆる Suzuki 群の発見があり, また本章の目標の一つである Frobenius 群の Frobenius 核の巾零性が Thompson により証明されたのである. Zassenhaus 群の完全な分類は, 近年の有限単純群論の出発点となる大切な結果なのであるが, その分類理論の完全な記述は, 伊藤昇著 "有限群論" (共立出版) にあるので, 興味のある読者は参照されたい. ——

さて, Frobenius 群の一般論に戻ろう. (G, N) を Frobenius 群, H をその Frobenius 補群とする. 補題 7.15 から, つぎのことがわかる:

(7.27) $$N_G(H) = H,$$

(7.28) $$H^{\sharp} \ni h \Longrightarrow C_G(h) \subseteqq H.$$

(7.27) は (7.26) から明らかであろう. $H^{\sharp} \ni h$, $C_G(h) \ni x$ とすると, $1 \neq h = h^x$

$\in H\cap H^x$ であるから，(7.26) により $x\in H$. すなわち (7.28) を得る.

$|N|=n$ とおく. (7.27) により，H は n 個の異なる共役 $H_1=H, H_2, \cdots, H_n$ をもつ. $H_0=N$ とおくと，(7.26) により

$$(7.29)\qquad G=\bigcup_{i=0}^{n}H_i,\qquad H_i\cap H_j=1\quad(i\neq j)$$

である.

さて，H, N については，

(α) H の N への作用の仕方,

(β) H の構造,

(γ) N の構造

について多くの大切な結果がある. 最初に (α) に対する解答を述べよう. (7.28) により

$$H^\sharp\ni h\Longrightarrow C_N(h)=1$$

であるから,

(7.30) $H^\sharp$ の各元は，N の上に単位元以外の固定点をもたない.

これが，(α) に対する解答である. 一般に群 A が群 X に作用しているとき，$C_X(A)=1$ ならば，A は X に**固定点なしに作用する**という. さらに，$A^\sharp\ni a$ が $C_X(a)=1$ なる条件を満たすとき，a は X に固定点なしに作用するという.

つぎの意味で (7.30) の逆が成り立つ.

補題 7.16 群 H が群 N に作用しているとき, $H^\sharp$ の各元が N に固定点なしに作用するならば，半直積 HN は Frobenius 群で N がその Frobenius 核である.

証明 $G=HN$ とおく. まず，G, H が (7.28) を満たすことを示そう. $H^\sharp\ni h$, $C_G(h)\ni x=kn\ (k\in H,\ n\in N)$ とすると,

$$kn=x=x^h=(kn)^h=k^hn^h\qquad(k^h\in H,\ n^h\in N)$$

より，$n=n^h$ すなわち $n\in C_N(h)$. 仮定より $n=1$. よって $x=k\in H$ すなわち G, H は (7.28) を満たす. このとき，補題 7.14 により $|H|$ と $|N|$ は互いに素であることがわかる. さて，$N\ni n\neq 1$, $C_G(n)\ni x$ のとき，$x\in N$ を示さねばならない. $N\not\ni x$ として矛盾を導こう.

$|H|=|G/N|$ と $|N|$ は互いに素であるから，x を適当なベキにとりかえることにより，x の位数は素数 p であるとしてよい. このとき，$p\mid |H|$ であるから

Sylow の定理により，G の或る元 y に対して $x^y \in H$. このとき，$n^y \in C_G(x^y) \subseteq H$. よって $n^y \in H \cap N = 1$ すなわち $n=1$ となり矛盾である. ▌

問 7.17 (G, N) を Frobenius 群，H をその Frobenius 補群とする. つぎの (i), (ii) を示せ:

(i) N_0 を H 不変な N の部分群とするとき，(HN_0, N_0) は Frobenius 群である. さらに H の部分群 $H_0 \neq 1$ に対して (H_0N, N) は Frobenius 群である.

(ii) $G \triangleright N_0 \subsetneqq N$ のとき，$(G/N_0, N/N_0)$ は Frobenius 群である.

[ヒント] 補題 7.16 の応用. (ii) に対しては定理 7.4 も用いる. ——

つぎの補題は，H, N の構造に対する部分的結果である.

補題 7.17 (G, N) を Frobenius 群，H をその Frobenius 補群とする. $|H|$ が偶数のとき，N は Abel 群で H はただ一つの位数 2 の元をもつ.

証明 $H^\sharp \ni \sigma$ とする. $N_\sigma = \{x^\sigma x^{-1} \mid x \in N\}$ とおけば，

$$\begin{aligned} x^\sigma x^{-1} = y^\sigma y^{-1} &\Longrightarrow (y^{-1}x)^\sigma = y^{-1}x \\ &\Longrightarrow y^{-1}x = 1 \qquad ((7.30) \text{ による}) \\ &\Longrightarrow x = y \end{aligned}$$

であるから，$|N_\sigma| = |N|$. すなわち N の各元は，$x^\sigma x^{-1}\,(x \in N)$ の形にただ 1 通りに書き表わせる. ここで σ を位数 2 の元としよう.

$$(x^\sigma x^{-1})^\sigma = x^{\sigma^2} x^{-\sigma} = x x^{-\sigma} = (x^\sigma x^{-1})^{-1}$$

であるから，すぐ上に示したことにより

$$N \ni y \Longrightarrow y^\sigma = y^{-1}$$

を得る. $N \ni y_1, y_2$ とすると

$$(y_1y_2)^\sigma = y_1{}^\sigma y_2{}^\sigma = y_1{}^{-1} y_2{}^{-1}, \quad (y_1y_2)^\sigma = (y_1y_2)^{-1} = y_2{}^{-1} y_1{}^{-1}$$

より，$y_1y_2 = y_2y_1$ となり N は Abel 群となる. τ を H の任意の位数 2 の元とすれば，τ に対しても $y^\tau = y^{-1}\ (\forall y \in N)$ であるから，$y^{\sigma\tau} = (y^{-1})^\tau = y\ (\forall y \in N)$ となり，(7.30) により $\sigma\tau = 1$. よって $\sigma = \tau^{-1} = \tau$ を得る. ▌

この補題の証明の中で示されたつぎの事実も大切である.

補題 7.18 有限群 N が位数 2 の固定点のない自己同型 σ をもてば，$y^\sigma = y^{-1}$ $(\forall y \in N)$ であり，N は Abel 群である. ——

H を Frobenius 群 (G, N) の Frobenius 補群とするとき，$|H|$ が偶数ならば，補題 7.17 により N は Abel 群 (とくに巾零群) となり，N は簡単な構造をもつ

が，H の構造を調べるのは難しい．それに反して，$|H|$ が奇数のときは，§7.3, c) で見るように H は比較的簡単な構造をもつが，N の巾零性の証明は難しい．しかし一般に Frobenius 補群の性質を調べるためにはつぎの定理7.9が基本的である．

定理 7.9 H を Frobenius 群 (G, N) の Frobenius 補群とするとき，H の位数 pq (p, q は必ずしも異ならない素数) の部分群は巡回群である．——

定理7.9の証明の前に一つの補題を述べておこう．

補題 7.19 G, N, H を定理7.9の通りとする．G が Abel 群 V に作用しているとき，$|N|$ と $|V|$ が互いに素ならば，$C_V(H)\neq 1$ または $C_V(N)\neq 1$ である．

証明 $|N|=n$ とおく．$H=H_1, H_2, \cdots, H_n$ を H の n 個の異なる共役とすると，(7.29) により

$$(7.31)\qquad G=\bigcup_{i=0}^{n} H_i,\qquad H_i\cap H_j=1\quad (i\neq j)\qquad (H_0=N \text{ とする})$$

である．以下，$C_V(H)=1$，$C_V(N)=1$ と仮定して矛盾を導こう．このとき，明らかに

$$(7.32)\qquad C_V(H_i)=1\qquad (i=0, 1, 2, \cdots, n)$$

である．$V\ni v\neq 1$ とすると

$$\prod_{x\in G} v^x,\ \prod_{x\in H_i} v^x \in C_V(H_i)\quad (i=0, 1, 2, \cdots, n)$$

であるから，(7.32) により

$$\prod_{x\in G} v^x=1,\qquad \prod_{x\in H_i} v^x=1$$

である．したがって (7.31) を用いれば，

$$\prod_{i=0}^{n}\prod_{x\in H_i} v^x = v^n \prod_{x\in G} v^x$$

となるから，$v^n=1$ を得る．しかるに $n=|N|$ と $|V|$ は互いに素であるから，$v^n=1$ より $v=1$ となり矛盾である．▌

定理 7.9 の証明 A を H の位数 pq の部分群とする．$p=q$ のとき A が巡回群でなければ，A は (p, p) 型の Abel 群である．このとき，定理7.7により

$$N=\langle C_N(a)\mid a\in A^\sharp\rangle$$

であるから，或る $a\in A^\sharp$ に対して $C_N(a)\neq 1$．これは，(7.30) に矛盾する．つぎ

に $p \neq q$ とする．A が巡回群でなければ，A は Frobenius 群である．$p<q$ とすると A の位数 q の部分群 A_q が Frobenius 核で位数 p の部分群 A_p が Frobenius 補群である．N の A 不変極小部分群を V とすると，問 7.10 により V は Abel 群で，$|H|$ と $|N|$ は互いに素であるから，$|V|$ は q と素である．このとき，補題 7.19 の G, N, H, V として，A, A_q, A_p, V をとれば，$C_V(A_p) \neq 1$ または $C_V(A_q) \neq 1$ を得る．これは (7.30) に矛盾している．▌

定理 7.9 は，Frobenius 補群の S_p 部分群は，位数 p の部分群をただ一つしか含まないことを示している．このような性質をもった p 群については，つぎのことが知られている．

補題 7.20　P を位数 p の部分群をただ一つしか含まないような p 群とする．このとき，

(i)　$p \neq 2$ ならば，P は巡回群，

(ii)　$p=2$ ならば，P は巡回群または 4 元数型の群(例 1.14 参照)

である．——

この補題と定理 7.9 から直ちにつぎの定理が得られる．

定理 7.10　Frobenius 群の Frobenius 補群の Sylow 部分群は，巡回群または 4 元数型の 2 群である．——

補題 7.20 の証明　最初に $p \neq 2$ のとき，P は巡回群であることを示そう．P を最小位数の反例とする．P は少なくとも二つの指数 p の部分群をもつ．実際，指数 p の部分群をただ一つしか含まないならば，それを Q とするとき $Q=\Phi(P)$．このとき $P-Q \ni x$ をとると，$P=\langle x, Q\rangle=\langle x, \Phi(P)\rangle=\langle x\rangle$ すなわち P は巡回群となり矛盾である．P_1, P_2 を P の指数 p の異なる部分群としよう．P は最小位数の反例だから，P_1, P_2 は巡回群である．また

$$P = P_1P_2 \rhd P_i \qquad (i=1,2)$$

である．さらに P は巾零クラスが 2 の p 群である．実際，$P \rhd P_i$ $(i=1,2)$ より $[P_1, P_2] \subseteqq P_1 \cap P_2 \lhd P$ で，明らかに $P/[P_1, P_2]$ は Abel 群であるから，$P' \subseteqq [P_1, P_2] \subseteqq P_1 \cap P_2$．一方，$P=P_1P_2$ より，明らかに $P_1 \cap P_2 \subseteqq Z(P)$．よって $P' \subseteqq Z(P)$ すなわち P の巾零クラスは 2 である．$P_1=\langle x\rangle$，$P_2=\langle y\rangle$ としよう．$x^p \in P_2$ だから，$x^p=y^p$ と仮定してよい．このとき，問 5.7 により

$$(xy^{-1})^p = x^py^{-p}[y, x]^{p(p-1)/2} = [y^p, x]^{(p-1)/2} = [x^p, x]^{(p-1)/2} = 1$$

となり，P が位数 p の部分群を少なくとも二つもつことになり矛盾である．

$p=2$ としよう．まず，位数 2^{n+1} $(n\geqq 2)$ の4元数型の群 $Q_{2^{n+1}}$ についてつぎの注意をしておこう：

（＊）$Q_{2^{n+1}}$ は，$n\geqq 3$ のときただ一つの指数2の巡回部分群を含み，$n=2$ のときは，ちょうど3個の指数2の巡回部分群を含む，

（＊＊）$\langle x\rangle$ を $Q_{2^{n+1}}$ の指数2の巡回部分群とすると，$Q_{2^{n+1}}-\langle x\rangle\ni y$ のとき，$x^y=x^{-1}$.

P をやはり最小位数の反例としよう．最初に P が指数2の巡回部分群を含むことを示そう．P_1 を P の指数2の部分群とする．P は最小位数の反例だから，P_1 が巡回群でなければ，P_1 は4元数型の群である：

$$P_1=\langle x, y\,|\,x^{2^{n-1}}=1,\ y^2=x^{2^{n-2}},\ x^y=x^{-1}\rangle \qquad (n\geqq 3).$$

$P-P_1\ni z$ をとると，上の注意（＊）により，z は $\langle x\rangle$ を不変にすると仮定してよい．このとき，$\langle x, z\rangle$ も P の指数2の部分群である．なぜならば，$P=\langle x, z\rangle$ とすると，$z^2\in P_1-\langle x\rangle$ となり，$x^z=x^a$ $(1\leqq a<2^{n-1})$ とおくと，（＊＊）により $x^{a^2}=x^{z^2}=x^{-1}$．よって $a^2\equiv -1 \pmod{2^{n-1}}$ $(n\geqq 3)$ を得るが，この合同式は成り立たないから，矛盾である．したがって，$P_2=\langle x, z\rangle$ も P の指数2の部分群であるが，P_2 が巡回群でなければ，P_2 も4元数型の群でなければならない．このとき（＊＊）により $x^z=x^{-1}$ であるから，$x^{yz}=x$ となり，$\langle x, yz\rangle$ は P の指数2の可換部分群である．しかるに P は位数2の元をただ一つしか含まないから，$\langle x, yz\rangle$ は巡回群でなければならない．以上により，P は指数2の巡回部分群を含むことがわかった．それをあらためて $\langle x\rangle$ としよう．$P-\langle x\rangle\ni y$ をとる．このとき，$y^2\in\langle x\rangle$ で，y は $\langle x\rangle$ の上に位数2の自己同型をひき起す．$\boldsymbol{Z}_{2^n}{}^*$ の位数2の元は

$$-1, \qquad -1+2^{n-1}, \qquad 1+2^{n-1} \pmod{2^n} \qquad (n\geqq 3)$$

であるから

$$x^y=x^{-1},\ x^{-1+2^{n-1}}\ \text{または}\ x^{1+2^{n-1}},$$
$$y^2=x^a\neq 1 \qquad (1\leqq a\leqq 2^n)$$

を得る．ただし $n=2$ のときは $x^y=x^{-1}$ の場合だけが起る．$x^y=x^{-1}$ とすると，$x^a=y^2=y^{-1}y^2y=(x^a)^y=x^{-a}$ より，$a=2^{n-1}$．したがって P は4元数型の群となり矛盾である．$x^y=x^{-1+2^{n-1}}$ とすると，同様にして $a=2^{n-1}$ を得るが，このと

き $(yx^{-1})^2=yx^{-1}yx^{-1}=y^2x^{1-2^{n-1}}x^{-1}=x^{2^{n-1}}x^{1-2^{n-1}}x^{-1}=1$ となり，P が位数 2 の部分群をただ一つしかもたないことに反する．最後に $x^y=x^{1+2^{n-1}}$ とする．このとき，$x^a=y^2=y^{-1}y^2y=x^{a+2^{n-1}a}$ より $a=2b$，$(2^{n-2}-1)i\equiv b \pmod{2^{n-1}}$ によって i を定めれば，$(yx^i)^2=yx^iyx^i=y^2x^{i+2^{n-1}i}x^i=x^{2^{n-1}i-2i}x^{2i+2^{n-1}i}=1$ となり，やはり矛盾である．▌

問 7.18 q を $SL(2,p)$ (p は奇素数) の位数を割る素数とする．$SL(2,p)$ の S_q 部分群は，

(i) $q\neq 2$ ならば，巡回群，

(ii) $q=2$ ならば，4 元数型の群

であることを示せ．また $SL(2,p)$ の可換部分群は巡回群であることを示せ．——

上の問 7.18 により，$SL(2,p)$ はその Sylow 部分群について，Frobenius 補群と全く同じ性質をもつことがわかる．しかし，$SL(2,p)$ が Frobenius 補群となるのは，$p=3,5$ のときに限ることが知られている．

§7.3 移送定理

有限群 G と素数 p が与えられたとき，G が指数 p の正規部分群をもつための条件を G の S_p 部分群との関係で調べることは，有限群論において大切である．本節では，この問題に対する結果のうち，いくつかの p 巾零性定理——Frobenius の定理 7.13，Burnside の定理 7.14，Thompson の定理 7.15——を取り上げる．これらは，有限群論において移送定理 (transfer theorems) と総称されている多くの結果の一部である．また§7.3, a) で証明される定理 7.11 と§7.3, b) で述べる Alperin の定理は，これら多くの移送定理に対して基本的役割を果たす．なお，Thompson の定理 7.15 は，§7.3, e) で証明される "Frobenius 群の Frobenius 核の巾零性" の証明の鍵となるものである．

a) 移　送

G を任意の群 (無限群でもよい)，H を G の指数有限の部分群，H^* は H の正規部分群で剰余群 H/H^* が Abel 群であるようなものとする．G の H による右剰余類の代表系 T をとり固定しよう：

$$G=\sum_{t\in T}Ht.$$

このとき G の元 x は

$$x=ht \qquad (h\in H,\ t\in T)$$

と一意的に書けるから，G から H への写像 η_T を

$$\eta_T(x) = h$$

によって定める．さらに η_T を用いて G から H/H^* への写像 V を

$$V(x) = \left(\prod_{t \in T} \eta_T(tx)\right) H^*$$

によって定義する．ここで H/H^* は Abel 群だから，右辺の積の順序は任意でよいことに注意せよ．この写像 V を G から H/H^* への**移送** (transfer) という．

補題 7.21　(i)　V は G から H/H^* への準同型である．

(ii)　V は，その定義に用いた $H\backslash G$ の代表系 T のとり方によらない．

証明　(i)　$G \ni x, y$ をとる．$t \in T$ に対して

$$tx = \eta_T(tx) t_x \tag{7.33}$$

によって $t_x \in T$ がただ一つ定まり，t が T のすべての元を走れば t_x も T の元全体を走る．また (7.33) により $txy = \eta_T(tx) t_x y$ であるから，

$$\eta_T(txy) = \eta_T(tx) \eta_T(t_x y)$$

を得る．したがって

$$\begin{aligned} V(xy) &= \left(\prod_t \eta_T(txy)\right) H^* = \left(\prod_t \eta_T(tx) \eta_T(t_x y)\right) H^* \\ &= \left(\prod_t \eta_T(tx)\right) H^* \left(\prod_t \eta_T(t_x y)\right) H^* \\ &= V(x) V(y) \end{aligned}$$

を得る．

(ii)　T, T' を $H\backslash G$ の二つの代表系とする．$Ht = Ht'$ のとき

$$t' = h_t t$$

なる $h_t \in H$ が定まる．$x \in G$ とすると

$$\begin{aligned} t'x &= \eta_{T'}(t'x) t_x' && (t_x' \in T'), \\ tx &= \eta_T(tx) t_x && (t_x \in T), \\ t_x' &= h_{t_x} \cdot t_x && (h_{t_x} \in H) \end{aligned}$$

であるから，$t'x = h_t tx$ を用いて

$$\eta_{T'}(t'x) h_{t_x} = h_t \eta_T(tx)$$

を得る．したがって

$$\left(\prod_{t'} \eta_{T'}(t'x)\right) H^* = \left(\prod_t h_t \eta_T(tx) h_{t_x}{}^{-1}\right) H^*$$

$$= \left(\prod_t \eta_T(tx)\right)H^*\left(\prod_t h_t\right)H^*\left(\prod_t h_{t_x}{}^{-1}\right)H^*.$$

ところで t が T のすべての元を走るとき，t_x も T の元全体を走るから，

$$\left(\prod_t h_t\right)H^* = \left(\prod_t h_{t_x}\right)H^*.$$

したがって，

$$\left(\prod_{t'} \eta_{T'}(t'x)\right)H^* = \left(\prod_t \eta_T(tx)\right)H^*$$

を得る．▌

$G \ni x$ に対して $V(x)$ を計算するとき，つぎのようにすることがある．$H\backslash G$ への x の作用が，長さ $r_1, r_2, \cdots$ の巡回置換の積に分解したとしよう：

$$(Ht_1\ Ht_1x\ \cdots\ Ht_1x^{r_1-1})(Ht_2\ Ht_2x\ \cdots\ Ht_2x^{r_2-1})\cdots.$$

このとき

$$t_1,\ t_1x,\ \cdots,\ t_1x^{r_1-1},\ t_2,\ t_2x,\ \cdots,\ t_2x^{r_2-1},\ \cdots$$

を $H\backslash G$ の代表系にとれば，$\eta(tx)$ の値は

$$1,\ 1,\ \cdots,\ t_1x^{r_1}t_1{}^{-1},\ 1,\ 1,\ \cdots,\ t_2x^{r_2}t_2{}^{-1},\ \cdots$$

となるから，

$$(7.34)\qquad V(x) = \left(\prod_i t_ix^{r_i}t_i{}^{-1}\right)H^*, \qquad \sum_i r_i = [G:H]$$

を得る．

つぎに進むために記号と言葉を定義しよう．

H を G の部分群とする．$H \ni x, y$ に対して

$$g^{-1}xg = y \qquad (\exists g \in G)$$

なる関係は H の上の同値関係である．この同値類を H の G **共役類**という．また $G \ni x, y$ に対して $h^{-1}xh=y$ なる $h \in H$ が存在するとき，

$$x \underset{H}{\sim} y$$

と書く．とくに $x \underset{G}{\sim} y$ は，x と y が G の同じ共役類に属することを示している．このときは簡単に(G を省略して) $x \sim y$ と書くこともある．最後に群 X の交換子群を以後 X' で表わす．

定理 7.11 有限群 G とその S_p 部分群 P に対して

$$P\cap G' = \langle x^{-1}y \mid x, y\in P,\ x \underset{G}{\sim} y\rangle$$

が成り立つ．――

定理 7.11 を証明する前にその意味を説明しておこう．一般に有限群 G と素数 p に対して

$$G/N \quad \text{が} \quad \text{可換 } p \text{ 群}$$

であるような最小の正規部分群 N が存在する．なぜならば $G/N_i\,(i=1,2)$ が可換 p 群ならば $G/N_1\cap N_2$ もそうだからである．そのような N を $G'(p)$ で表わそう．このとき明らかに

$$G'(p)\supseteqq G', \qquad [G'(p):G'] \text{ は } p \text{ と素}$$

であるから

$$P\cap G'(p) = P\cap G' \tag{7.35}$$

を得る．さらに $G=PG'(p)$ であるから

$$G/G'(p)\simeq P/P\cap G'(p) = P/P\cap G'. \tag{7.36}$$

ところで上の定理 7.11 は，P の G 共役類がわかれば $P\cap G'$ が定まることを示している．したがって (7.36) は，P の G 共役類が，$G/G'(p)$ の構造を決定することを示す．とくに P の G 共役類がわかれば，G が指数 p の正規部分群をもつかどうかがわかるわけである．

定理 7.11 の証明　$P^*=\langle x^{-1}y \mid x\underset{G}{\sim}y,\ x, y\in P\rangle$ とおく．$x\underset{G}{\sim}y$ $(x, y\in P)$ ならば，$y=z^{-1}xz\ (\exists z\in G)$ であるから $x^{-1}y=x^{-1}z^{-1}xz=[x, z]\in G'\cap P$，よって $P^*\subseteqq P\cap G'$ である．また $P'\subseteqq P^*$ であるから，P/P^* は Abel 群である．$P^*\supseteqq P\cap G$ を示すためには，G から P/P^* への移送 V が全射であることを示せばよい．なぜならば，K を V の核とするとき V が全射ならば $G/K\simeq P/P^*$．したがって，(7.35) により $P\cap K\supseteqq P\cap G'\supseteqq P^*$．一方，$[G:K]=[P:P\cap K]=[P:P^*]$ より $|P\cap K|=|P^*|$．したがって $P\cap G'\subseteqq P\cap K=P^*$ となるからである．以下 V が全射であることを示そう．

$P\ni x$ に対して $V(x)$ を (7.34) を用いて計算すると

$$V(x) = \Bigl(\prod_i t_i x^{r_i} t_i^{-1}\Bigr)P^* = \Bigl(\prod_i x^{r_i}(x^{-r_i}t_i x^{r_i} t_i^{-1})\Bigr)P^*,$$

$$n = [G:P] = \sum_i r_i.$$

ところで P^* の定義により $x^{-r_i}t_ix^{r_i}t_i^{-1}\in P^*$ であるから

$$V(x) = x^{\Sigma r_i}P^* = x^nP^*$$

を得る．$n=[G:P]$ は p と素だから，$V(x)=x^nP^*$ は $V(P)=P/P^*$ を示す．とくに V は全射である．▌

問 7.19 $P\in \mathrm{Syl}_2(G)$，M を P の指数 2 の部分群とする．P の位数 2 の或る元が M のどの元とも G で共役でないならば，G は指数 2 の正規部分群をもつ．

[ヒント] x を仮定を満たす位数 2 の元として，G から P/M への移送 V を計算し $V(x)\neq 1$ を見ればよい．この問は Thompson の移送補題として有名である．

b) Alperin の定理

a) で G が指数 p の正規部分群をもつかどうかを知るには G の S_p 部分群 P の G 共役類を定めればよいことがわかった．それでは，P の G 共役類はどのようにして定まるのであろうか．この問に対するもっとも一般的な解答を与えるのがつぎに述べる Alperin の定理である．有限群 G とその S_p 部分群 P を固定する．P の部分群 T で $N_P(T)\in \mathrm{Syl}_p(N_G(T))$ なるものの全体を $\mathscr{F}$ で表わそう：

$$\mathscr{F} = \{T\subseteqq P \mid N_P(T)\in \mathrm{Syl}_p(N_G(T))\}.$$

定理 7.12 (Alperin) A, B は P の部分集合で，或る $x\in G$ に対して

$$A^x = B$$

とする．このとき，$\mathscr{F}\ni T_1, T_2, \cdots, T_n$ と $N_G(T_i)\ni x_i\ (i=1,2,\cdots,n)$ が存在して，

(α) $A\subseteqq T_1$, $\quad A^{x_1x_2\cdots x_i}\subseteqq T_{i+1}\quad (1\leqq i\leqq n-1)$,

(β) $x = x_1x_2\cdots x_n$

である．とくに P の G 共役類は $\mathscr{F}$ の各元 T の $N_G(T)$ 共役類によって定まる．——

定理の証明に入る前に一つの補題と記号の準備をしよう．

補題 7.22 T を P の任意の部分群とするとき，T の或る共役は $\mathscr{F}$ に含まれる．

証明 $N_P(T)\subseteqq Q\in \mathrm{Syl}_p(N_G(T))$, $Q\subseteqq P_0\in \mathrm{Syl}_p(G)$ なる Q, P_0 をとる．Sylow の定理により $P_0{}^x=P$ なる $x\in G$ が存在する．このとき $T^x\in\mathscr{F}$ を見るのはやさしい．▌

A, B は P の部分集合で，$A^x=B$ $(x\in G)$ のとき，定理 7.12 の結論 (α), (β) を満たす $\mathscr{F}\ni T_1, \cdots, T_n$ と $N_G(T_i)\ni x_i$ が存在するならば

$$A \underset{x}{\longrightarrow} B$$

と書くことにしよう．このとき，

(7.37) $$A \underset{x}{\longrightarrow} B, \quad A \supseteqq C \Rightarrow C \underset{x}{\longrightarrow} C^x,$$

(7.38) $$A \underset{x}{\longrightarrow} B, \quad B \underset{y}{\longrightarrow} C \Rightarrow A \underset{xy}{\longrightarrow} C$$

が成り立つことが容易にわかる．

問 7.20 (7.37), (7.38) を確かめよ．

定理 7.12 の証明 まず A, B は P の部分群としてよいことに注意する．なぜならば $T=\langle A\rangle$ とおくと $T^x=\langle B\rangle$ だから，部分群に対して定理が正しければ $T \underset{x}{\longrightarrow} T^x$．このとき (7.37) により $A \underset{x}{\longrightarrow} A^x=B$ となるからである．したがって以下 A, B は P の部分群としよう．$[P:A]$ に関する数学的帰納法により証明する．$[P:A]=1$ すなわち $P=A$ ならば，$P=B=A^x=P^x$ より $x \in N_G(P)$．よって $T_1=P$, $x_1=x$ とすれば定理が成り立つ．つぎに $[P:A]>1$ としよう．$A_1=N_P(A)$, $B_1=N_P(B)$ とおけば，定理 5.1 により

(7.39) $$A_1 \supsetneqq A, \qquad B_1 \supsetneqq B$$

である．補題 7.22 により $N_P(B^{x_1}) \in \mathrm{Syl}_p(N_G(B^{x_1}))$ なる $x_1 \in G$ が存在する．このとき

$$A^{xx_1} = B^{x_1} = C$$

とおくと，$C \in \mathscr{F}$ である．$N_P(A)^{xx_1} \subseteqq N_G(A^{xx_1})=N_G(C)$, かつ $N_P(C) \in \mathrm{Syl}_p(N_G(C))$ より，$x_2 \in N_G(C)$ が存在して $N_P(A)^{xx_1x_2} \subseteqq N_P(C) \subseteqq P$．よって $x_1x_2=y$ とおくと，

(7.40) $$A^{xy} = B^y = C, \qquad {A_1}^{xy} \subseteqq P$$

を得る．同様に $N_P(B)^{x_1} \subseteqq N_G(B^{x_1})=N_G(C)$, かつ $N_P(C) \in \mathrm{Syl}_p(N_G(C))$ より，$x_3 \in N_G(C)$ が存在して $B^{x_1x_3} \subseteqq N_P(C) \subseteqq P$．よって $x_1x_3=z$ とおいて

(7.41) $$B^z = C, \qquad {B_1}^z \subseteqq P$$

を得る．(7.40), (7.41) の最初の等式から，$B^y=B^z=C \in \mathscr{F}$, $y^{-1}z \in N_G(C)$ であるから，

(7.42) $$B^y \underset{y^{-1}z}{\longrightarrow} B^z$$

である．一方，(7.39) により $[P:A_1]<[P:A]$, $[P:B_1]<[P:B]$ だから，帰納法の仮定と (7.39), (7.40) から

$$A_1 \xrightarrow[xy]{} A_1{}^{xy}, \qquad B_1{}^z \xrightarrow[z^{-1}]{} B_1.$$

したがって(7.37)により

(7.43) $$A \xrightarrow[xy]{} A^{xy} = B^y, \qquad B^z \xrightarrow[z^{-1}]{} B.$$

このとき，(7.42), (7.43), (7.38)から $A \xrightarrow[x]{} B$ を得る．▌

Alperinの定理は，$\mathscr{F}$ の各元 T に対して T の $N_G(T)$ 共役類がわかれば，P の G 共役類がわかることを示している．しかし P が特別な場合には，P の G 共役類がもっと簡単にわかることもある．つぎの補題は有名である．

補題 7.23 (Burnside) $\mathrm{Syl}_p(G) \ni P$ を Abel 群とする．A, B は G で共役な P の部分集合とすると，或る $u \in N_G(P)$ が存在して $A^u = B$ である．とくに P の G 共役類は P の $N_G(P)$ 共役類と一致する．

証明 P は Abel 群だから，$C_G(A) \supseteq P$, $C_G(B) \supseteq P$. 一方，仮定により

$$A^x = B \qquad (\exists x \in G).$$

よって $C_G(B) = C_G(A)^x \supseteq P^x$ であるから，P^x, P は $C_G(B)$ の S_p 部分群である．したがって Sylow の定理により $C_G(B) \ni y$ が存在して

$$P^{xy} = P \quad \text{すなわち} \quad xy \in N_G(P).$$

また $A^{xy} = B^y = B$. よって $u = xy$ が求めるものである．▌

問 7.21 G を有限群，p を素数，$P \in \mathrm{Syl}_p(G)$ とする．$Z(P)$ の G 共役類は，$Z(P)$ の $N_G(P)$ 共役類と一致することを示せ．[ヒント] 補題7.23の証明の真似をせよ．

c) Frobenius の定理と Burnside の定理

有限群 G が，

$$G \triangleright K, \qquad |K| \text{ は } p \text{ と素}, \qquad [G:K] \text{ は } p \text{ のベキ}$$

なる正規部分群 K をもつとき，G を **p 巾零群**，K を G の**正規 p 補群**という．G が p 巾零群のとき，$P \in \mathrm{Syl}_p(G)$, K を正規 p 補群とするとき，

$$G = PK, \qquad P \cap K = 1$$

である．つぎの(7.44), (7.45)は定義から直ちに得られる：

(7.44) G が p 巾零であるためには，G の位数が p と素な元全体が G の部分群であることが必要十分である，

(7.45) G が p 巾零ならば，G の部分群や剰余群は p 巾零である．

問 7.22　(7.44), (7.45) を証明せよ.

問 7.23　G を有限群, p を素数とする. $q \neq p$ なる各素数 q に対して, G が q 巾零ならば G の S_p 部分群は正規部分群であることを示せ. [ヒント] $q \neq p$ なる各素数に対して正規 q 補群をとり, 補題 7.11 を用いる.

問 7.24　有限群 G が巾零であるためには, G の位数を割る各素数 p に対して p 巾零であることが必要十分であることを示せ.

定理 7.13(Frobenius)　G を有限群, $P \in \mathrm{Syl}_p(G)$ とするとき, つぎの条件は同値である:

(i)　G は p 巾零,

(ii)　P の各部分群 $T \neq 1$ に対して $N_G(T)$ は p 巾零,

(iii)　P の各部分群 $T \neq 1$ に対して $N_G(T)/C_G(T)$ は p 群,

(iv)　$P \ni x, y$ に対して

$$x \underset{G}{\sim} y \Longrightarrow x \underset{P}{\sim} y,$$

すなわち P の G 共役類と P の共役類とは一致する.

証明　(i) $\Longrightarrow$ (ii) は (7.45) から明らかであるから (ii) $\Longrightarrow$ (iii) を示そう. $Q \in \mathrm{Syl}_p(N_G(T))$ とすると, 仮定 (ii) により $N_G(T) = QK_0 \rhd K_0$, $Q \cap K_0 = 1$ なる $N_G(T)$ の部分群 K_0 が存在する. このとき, $[K_0, T] \subseteq K_0 \cap T = 1$ すなわち $K_0 \subseteq C_G(T)$. よって

$$N_G(T) = QC_G(T).$$

これは, $N_G(T)/C_G(T)$ が p 群であることを示している.

(iii) $\Longrightarrow$ (iv): Alperin の定理 7.12 を用いる. $a, b \in P$, $a^x = b$ $(x \in G)$ とする. Alperin の定理により,

$$\mathscr{F} \ni T_1, T_2, \cdots, T_n \quad \text{と} \quad N_G(T_i) \ni x_i$$

が存在して

$$a \in T_1, \qquad a^{x_1 x_2 \cdots x_i} \in T_{i+1}, \qquad x = x_1 x_2 \cdots x_n$$

となる. $a^{x_1 x_2 \cdots x_i} = a_i$ とおくと $a_i^{x_{i+1}} = a_{i+1}$, $x_{i+1} \in N_G(T_{i+1})$ である. ところで仮定 (iii) により $N_G(T_{i+1})/C_G(T_{i+1})$ は p 群で, $N_P(T_{i+1}) \in \mathrm{Syl}_p(N_G(T_{i+1}))$ であるから,

$$N_G(T_{i+1}) = N_P(T_{i+1}) C_G(T_{i+1}).$$

したがって

$$x_{i+1} = x_{i+1}'x_{i+1}'', \qquad x_{i+1}' \in N_P(T_{i+1}), \qquad x_{i+1}'' \in C_G(T_{i+1})$$

と書くと,

$$a_{i+1} = a_i^{x_{i+1}} = a_i^{x_{i+1}'x_{i+1}''} = a_i^{x_{i+1}'}.$$

よって $a_i \underset{P}{\sim} a_{i+1}$ である．したがって $a \underset{P}{\sim} a_1 \underset{P}{\sim} a_2 \underset{P}{\sim} \cdots \underset{P}{\sim} a_n = b$ すなわち $a \underset{P}{\sim} b$ を得る．

(iv) $\Longrightarrow$ (i)：K を G の位数が p と素な元の全体で生成される G の部分群とする．K は指数 p の正規部分群をもたない．なぜならば $[K:K_0]=p$, $K \triangleright K_0$ ならば，G の位数が p と素な元は K_0 に含まれてしまうからである．(i) を示すには $K \cap P = 1$ をいえばよいから，$T = K \cap P \neq 1$ と仮定して矛盾を出そう．P の昇中心列 $Z_k(P)$ $(k=0,1,2,\cdots)$ において，$Z_k(P) \not\supseteq T$, $Z_{k+1}(P) \supseteq T$ なる k をとり，$Z_k(P) = N$ とおくと,

$$T \subsetneqq N, \qquad [T,P] \subseteqq N$$

である．$T \in \mathrm{Syl}_p(K)$ であるから，定理 7.11 により

$$T \cap K' = \langle x^{-1}y \mid x \underset{K}{\sim} y,\ x, y \in T \rangle.$$

ところで仮定 (iv) により $x \underset{K}{\sim} y$ ならば，$x \underset{P}{\sim} y$ すなわち $u \in P$ が存在して $x^u = y$ であるから

$$x^{-1}y = x^{-1}x^u = [x,u] \in [T,P] \subseteqq N.$$

したがって

$$T \cap K' \subseteqq T \cap N \subsetneqq T.$$

これは K が指数 p の正規部分群をもつことを示すから，矛盾である．▌

定理 7.14 (Burnside)　$\mathrm{Syl}_p(G) \ni P$ が，$N_G(P) = C_G(P)$ なる条件を満たすとする．このとき G は p 巾零である．

証明　$P \subseteqq N_G(P) = C_G(P)$ であるから，P は Abel 群である．よって補題 7.23 により，P の G 共役類は P の $N_G(P)$ 共役類と一致する．ところで仮定 $N_G(P) = C_G(P)$ により，P の $N_G(P)$ 共役類は P の共役類に一致するから，結局 P の G 共役類は P の共役類と一致する．このとき，定理 7.13 の (iv) により G は p 巾零である．▌

例題 7.5　$\mathrm{Syl}_p(G) \ni P$ を巡回群とする．つぎの条件の一つが成り立つとき,

G は p 巾零である:

(i) p は $|G|$ を割る最小の素数,

(ii) G は指数 p の正規部分群をもつ.

[証明] (i) $N_G(P)/C_G(P)$ は P の全自己同型群 $\mathrm{Aut}(P)$ の部分群と同型であり, また $P \subseteqq C_G(P)$ であるから $N_G(P)/C_G(P)$ の位数は p と素である. $|\mathrm{Aut}(P)| = p^{n-1}(p-1)$ ($|P|=p^n$) であるから, $|N_G(P)/C_G(P)| \mid p-1$. しかるに p は $|G|$ を割る最小の素数だから, $|N_G(P)/C_G(P)|=1$ すなわち $N_G(P)=C_G(P)$. したがって定理7.14により G は p 巾零である. (ii) Schur-Zassenhaus の定理により $N_G(P)/P$ は補群 H をもつ. $[H,P] \subseteqq P \cap G'$ であるから, (ii) の仮定と定理7.11により

$$[H,P] \subseteqq P \cap G' \subsetneqq P.$$

P は巡回群であるから $P \cap G' \subseteqq \Phi(P)$. よって $[H,P] \subseteqq \Phi(P)$. このとき, 補題7.12の (i) により $[H,P]=1$ を得る. したがって $N_G(P)=HP=C_G(P)$ となり, 定理7.14により G は p 巾零である. ▌

この例題により, 有限群 G の S_2 部分群が巡回群ならば G は2巾零である. さらに Feit-Thompson の定理を用いれば, そのような群は可解群であることがわかる. 近年, 2群が与えられたとき, それを S_2 部分群とする有限群の構造を決定するという問題について著しい進歩がなされているが, いま述べたのはそのような結果のもっとも原始的なものである.

例題 7.6 G は各素数に対して Sylow 部分群が巡回群であるような群とする. このとき

(i) $G', G/G'$ は巡回群,

(ii) $|G'|$ と $|G/G'|$ は互いに素

である. とくに G は可解群である.

[証明] まず G が可解群であることを示そう. p は $|G|$ を割る最小の素数とする. 例題7.5により G は p 巾零である. G の正規 p 補群を K とすると, K も G と同じ仮定を満たすから, 位数に関する数学的帰納法により K は可解群であると仮定してよい. このとき, K および G/K=巡回群の可解性から G の可解性がでる. N を G の極大可換正規部分群とする. $C_G(N)=N$ を示そう. そのために $C_G(N) \supsetneqq N$ と仮定して矛盾を出そう. $C_G(N)/N$ に含まれる G/N の極小正

規部分群を L/N とすると，L/N は Abel 群であり，しかも L/N の Sylow 部分群は巡回群だから L/N も巡回群である．このとき $[L,N]=1$ に注意すれば，L は Abel 群となる．$G\triangleright L$ であるから，これは N の極大性に反する．したがって $C_G(N)=N$ が示された[1]．このとき G/N は $\mathrm{Aut}(N)$ の部分群と同型であり，N は巡回群であるから $\mathrm{Aut}(N)$ は Abel 群，よって G/N も Abel 群である．したがって $N\supseteqq G'$．とくに G' は巡回群である．G/G' の Sylow 部分群はすべて巡回群だから，G/G' も巡回群でなければならない．これで (i) が示された．$p\,|\,|G/G'|$ なる素数 p をとる．例題 7.5 の (ii) により G は p 巾零だから，G の正規 p 補群を K とすれば $K\supseteqq G'$．これは p が $|G'|$ と素であることを示す．▌

位数 $p_1p_2\cdots p_r$ (p_i は異なる素数) の群は，明らかに例題 7.6 の仮定を満たす．また Frobenius 群の Frobenius 補群が奇数位数のとき，定理 7.10 によりそれは例題 7.6 の仮定を満たす．したがって奇数位数の Frobenius 補群は簡単な構造をもつ可解群である．

d) Thompson の p 巾零性定理

ここでは，Thompson により証明された一つの定理を取り上げる．これは，§7.3, e) で証明される "Frobenius 群の Frobenius 核の巾零性" の証明の鍵となるものである．なお，この定理は，現在では Glauberman によってもっと深められているが，それは §7.4, c) で述べられるであろう．しかし，ここで述べる Thompson の定理は，その内容の深さに比べて証明はそれ程多くの準備を必要としないという利点をもっている．またその証明は，現在の有限群論の手法が非常によく現われていると思われるので，熟読玩味されることを望む次第である．

p 群の Thompson 部分群の定義から始めよう[2]．P を群とする．P の可換部分群全体の集合を $\mathscr{A}(P)$ として

$$d=\max_{A\in\mathscr{A}(P)} m(A)$$

とおく．ここで $m(A)$ は A の生成元の最小個数を表わす．さらに

1) $F(G)$ を G の Fitting 部分群 (＝最大の巾零正規部分群) とするとき，$F(G)=N$ である．実際，$F(G)\supseteqq N$ は明らかであり，Sylow 部分群がすべて巡回群であることから $F(G)$ も巡回群，よって，$F(G)=N$ である．このとき $C_G(N)=N$ は定理 5.6 からもでる．

2) 最近では，Thompson 部分群の定義は，ここで述べるものと少し異なるものを用いている．それについては §7.4, c) を参照．

$$\mathscr{A}_m(P) = \{A \in \mathscr{A}(P) \mid m(A) = d\},$$
$$J(P) = \langle A \mid A \in \mathscr{A}_m(P) \rangle$$

とおく．$J(P)$ を P の **Thompson 部分群**という．定義から明らかに

(7.46) $\quad J(P) \subseteq Q = P$ の部分群 $\Longrightarrow J(P) = J(Q)$

である．また $J(P)$ は P の特性部分群であるから

(7.47) $\quad P$ が G の部分群 のとき $N_G(J(P)) \supseteq N_G(P)$

である．

定理 7.15 (Thompson) G を有限群，p を奇素数，$P \in \mathrm{Syl}_p(G)$ とする．$N_G(J(P))$ と $C_G(Z(P))$ が p 巾零ならば，G も p 巾零である．——

$p=2$ のとき，この定理は成立しない．実際，4 次対称群 $\mathfrak{S}_4$ は定理の仮定を満たすが結論は成立しない．このことは容易に確かめることができる．

問 7.25 これを確かめよ．——

しかし，この定理の証明の中で $p \neq 2$ なる仮定を用いるのは，証明の最終段階において一度だけである．そのときにつぎの補題を用いる．

補題 7.24 G を $SL(2,p)$ の位数 pq の非可換部分群とする (q は p と異なる素数)．G の S_q 部分群が G の正規部分群ならば，$p=2$, $q=3$ である．

証明 $p \neq 2$ と仮定する．このとき，p は $SL(2,p)$ の位数 $p(p^2-1)$ を割る最大の素数であるから，$p>q$ である．したがって G の S_p 部分群は，G の正規部分群である．G の S_q 部分群も G の正規部分群だから，G は巡回群となり，G が非可換部分群であることに反する．▌

定理 7.15 の証明 G を最小位数の反例とする．P の部分群の集合 $\mathscr{H}$ を

$$\mathscr{H} = \{T \subseteq P \mid T \neq 1,\ N_G(T) \neq p\ \text{巾零}\}$$

によって定義する．G は p 巾零でないから，Frobenius の定理 7.13 の (ii) により，$\mathscr{H}$ は空集合ではない．$\mathscr{H}$ の元 T で

$$|N_G(T)|_p \qquad (= N_G(T)\ \text{の}\ S_p\ \text{部分群の位数})$$

が最大になるもの全体を考え，その中でさらに

$$|T|\ \text{が最大になるもの}$$

を一つとり，それを H とする．$N_P(H) \in \mathrm{Syl}_p(N_G(H))$ と仮定してよい (補題 7.22)．以下，G の性質を段階に分けて調べ，矛盾を導こう．

(α) (i) H は G の最大の正規 p 部分群である．

(ii) $H \neq P$.

(iii) G/H は p 巾零.

(iv) G の正規 p' 部分群(位数が p と素な正規部分群)は単位群に限る.

[証明] (i) まず $G \triangleright H$ を示そう. それには, $N_G(H)$ が定理の仮定を満たすことをいえばよい. なぜなら, そのとき $G \neq N_G(H)$ ならば, G が最小位数の反例であることから $N_G(H)$ は p 巾零となり, $H \in \mathscr{H}$ に反するからである. $P^* = N_P(H)$ とおくと, $P^* \in \mathrm{Syl}_p(N_G(H))$ である. 明らかに $Z(P) \subseteq Z(P^*)$. よって $C_G(Z(P)) \supseteq C_G(Z(P^*))$ となり, $C_G(Z(P^*))$ は p 巾零である. $P^*=P$ ならば $N_G(J(P^*)) = N_G(J(P))$ は p 巾零となり, $N_G(H)$ は定理の仮定を満たす. よって $P^* \neq P$ としよう. このとき, (7.47) により $N_P(J(P^*)) \supseteq N_P(P^*) \supsetneqq P^*$ であるから, $|N_G(J(P^*))|_p > |P^*| = |N_G(H)|_p$ となり, H の選び方から $N_G(J(P^*))$ は p 巾零でなければならない. よって $P^* \neq P$ のときも $N_G(H)$ は定理の仮定を満たす. これで $G \triangleright H$ が示された. つぎに $G \triangleright H_1 \supsetneqq H$, $H_1 = p$ 群とすると, $G = N_G(H_1)$ は p 巾零でないから, $H_1 \in \mathscr{H}$. $H_1 \supsetneqq H$ であるから, やはり H の選び方に反する. 以上により (i) が示された.

(ii) $P=H$ ならば, (7.47) により $G = N_G(J(P))$. このとき, G は p 巾零となり矛盾である.

(iii) $\bar{G} = G/H$ とおく. $\mathrm{Syl}_p(\bar{G}) \ni \bar{P} = P/H$ である.

$$Z(\bar{P}) = Z(P/H) = Z^*/H, \qquad J(\bar{P}) = J(P/H) = J^*/H$$

とおくと, $P \neq H$ であるから,

$$Z^* \supsetneqq H, \qquad J^* \supsetneqq H$$

である. よって, $|N_G(J^*)|_p = |N_G(Z^*)|_p = |G|_p$ に注意すれば, H の選び方により, $N_G(Z^*)$, $N_G(J^*)$ は p 巾零である. 明らかに

$$N_{\bar{G}}(J(\bar{P})) = \overline{N_G(J^*)}, \qquad N_{\bar{G}}(Z(\bar{P})) = \overline{N_G(Z^*)}$$

であるから, $N_{\bar{G}}(J(\bar{P}))$, $N_{\bar{G}}(Z(\bar{P}))$ も p 巾零となる. これは, $\bar{G}$ が定理の仮定を満たすことを示している. よって $|\bar{G}| < |G|$ より, $\bar{G}$ は p 巾零でなければならない.

(iv) N を G の正規 p' 部分群としよう. $N \neq 1$ と仮定して矛盾を導く. $\bar{G} = G/N$ とおき, $\bar{G}$ が定理の仮定を満たすことを示そう. $|N|$ は p と素であるから, 自然準同型 $P \to \bar{P}$ は同型であり, したがって

$$Z(\bar{P}) = \overline{Z(P)}, \qquad J(\bar{P}) = \overline{J(P)}.$$

また補題7.10により

$$N_{\bar{G}}(\overline{J(P)}) = \overline{N_G(J(P))}, \qquad C_{\bar{G}}(\overline{Z(P)}) = \overline{C_G(Z(P))}$$

であるから，$N_{\bar{G}}(J(\bar{P}))=\overline{N_G(J(P))}$, $C_{\bar{G}}(Z(\bar{P}))=\overline{C_G(Z(P))}$ となり，$N_{\bar{G}}(J(\bar{P}))$, $C_{\bar{G}}(Z(\bar{P}))$ は p 巾零である．よって $\bar{G}$ は定理の仮定を満たすから，$N \neq 1$ ならば $\bar{G}$ が p 巾零となる．このとき，N の位数が p と素なことに注意すれば，G も p 巾零となり矛盾である．▌

(β)　$C_G(H) \subseteqq H$.

［証明］[1]　(α), (iii) により G/H は p 巾零であるから，G/H の正規 p 補群を Q/H とする．$L=Q \cap HC_G(H)$ とおき，$L=H$ を最初に示そう．明らかに $L \triangleright H$ である．また $[L:H]$ と $|H|$ は互いに素であるから，Schur-Zassenhaus の定理により L/H は補群 M をもつ．このとき，M は p' 部分群，H は p 群であるから，$M \subseteqq HC_G(H) \triangleright H$ より $M \subseteqq C_G(H)$ を得る．よって $L=MH=M \otimes H$ である．ところで明らかに $G \triangleright L$ であるから，$|M|$ と $|H|$ が互いに素であることに注意すれば $M \triangleleft G$ となり，(α), (iv) により $M=1$. したがって $L=H$ である．Q/H は G/H の正規 p 補群であったから，$L=H$ は $HC_G(H)$ が p 群であることを示す．$HC_G(H) \triangleleft G$ であるから，(α), (i) により $HC_G(H)=H$. すなわち $H \supseteqq C_G(H)$ である．▌

(γ)　(i)　P は G の極大部分群である．

(ii)　Q/H を G/H の正規 p 補群とすると，$\bar{Q}=Q/H$ は或る素数 q に対する基本 Abel 群，$\bar{P}=P/H$ は $\bar{Q}$ の上に忠実かつ既約に作用する．

［証明］　(i) $P \subsetneqq G_1 \subsetneqq G$ なる部分群 G_1 が存在したとする．G_1 は定理の仮定を満たすから，$|G_1|<|G|$ より G_1 は p 巾零である．K を G_1 の正規 p 補群とすると，$P \subsetneqq G_1$ より $K \neq 1$. また $G_1 \triangleright H$, $G_1 \triangleright K$ より $[H, K] \subseteqq H \cap K=1$ すなわち $K \subseteqq C_G(H)$ となり，これは (β) に矛盾する．(ii) $\bar{G}=G/H$, $\bar{P}=P/H$, $\bar{Q}=Q/H$ とおく．$\bar{P}$ は $\bar{Q}$ に素に作用していて，$\bar{P}$ は $\bar{G}=\bar{P}\cdot\bar{Q}$ の極大部分群であるから，問7.10により $\bar{Q}$ は或る素数 q に対する基本 Abel 群で，$\bar{P}$ は $\bar{Q}$ に既約に作用しなければならない．$\bar{P}$ の $\bar{Q}$ への作用の核を $\bar{H}_1=H_1/H$ とすると，$H_1 \triangleleft G$ で

1)　(β) は§7.4, a)，定理7.20からも得られる．(α) により G は p 可解群 (§7.4, a)) であることに注意せよ．また，ここで与える (β) の証明は，定理7.20の別証明でもある．

H_1 は p 群だから，(α), (i) によって $H_1=H$. よって $\bar{P}$ の $\bar{Q}$ への作用は忠実である. ▌

(δ) $\mathscr{A}_m(P)\ni A$ が存在して，$P=AH$. また $\bar{P}=P/H=\bar{A}$ は，巡回群である.

[証明] $J(P)\subseteqq H$ とすると，G の任意の元 x に対して $J(P)^x\subseteqq H\subseteqq P$ であるから，$J(P)\subseteqq P^{x^{-1}}$. よって $J(P)=J(P^{x^{-1}})=J(P)^{x^{-1}}$ すなわち $J(P)\lhd G$ である. このとき $G=N_G(J(P))$ が p 巾零となり矛盾である. したがって $J(P)\subsetneqq H$. これは或る $A\in\mathscr{A}_m(P)$ が存在して，$A\subsetneqq H$ なることを意味する. そこで $\bar{A}$ 不変な $\bar{Q}$ の部分群 $\bar{Q}_1=Q_1/H$ で，$\bar{A}$ は $\bar{Q}_1$ 上に既約かつ $[\bar{A},\bar{Q}_1]\neq 1$ なるものをとる ($\bar{P}$ の $\bar{Q}$ の上への作用の忠実性から，このような $\bar{Q}_1$ がとれることに注意). $G_1=AQ_1$ とおく. $G=G_1$ を示そう. G_1 が p 巾零ならば，その正規 p 補群を K とするとき，$K\subseteqq C_G(H)$ となり (β) に反する. よって G_1 は p 巾零ではない. したがって $G=G_1$ を示すには，G_1 が定理の仮定を満たすことをいえば十分である. $P_1=AH$ とおくと，$P_1\in \mathrm{Syl}_p(G_1)$ である. $Z(P)\subseteqq C_G(H)\subseteqq H\subseteqq P_1$ より $Z(P)\subseteqq Z(P_1)$. よって $C_G(Z(P))\supseteqq C_G(Z(P_1))$ となり，$C_G(Z(P_1))$ は p 巾零である. $N_{G_1}(J(P_1))$ の p 巾零性を見るために，$\mathrm{Syl}_q(N_{G_1}(J(P_1)))\ni Q_2$ とする. このとき，

$$[A, Q_2]\subseteqq[J(P_1), Q_2]\subseteqq J(P_1)$$

であるから，$[\bar{A},\bar{Q}_2]$ は p 群である. 一方

$$[\bar{A},\bar{Q}_2]\subseteqq[\bar{A},\bar{Q}]\subseteqq\bar{Q}_1$$

であるから，$[\bar{A},\bar{Q}_2]$ は q 群である. したがって $[\bar{A},\bar{Q}_2]=1$. $\bar{A}$ の $\bar{Q}_1$ への作用は既約で $[\bar{A},\bar{Q}_1]\neq 1$ であるから，$\bar{Q}_2=1$ を得る. これは，$N_{G_1}(J(P_1))$ が p 群であることを示すから，とくに $N_{G_1}(J(P_1))$ は p 巾零である. 以上によって，G_1 は定理の仮定を満たし，したがって $G=G_1$ であることがわかった. とくに $P=AH$ を得る. このとき，$\bar{P}=\bar{A}$ は Abel 群となり，$\bar{P}$ の $\bar{Q}$ への作用は忠実かつ既約であるから，補題 7.5 により $\bar{P}$ は巡回群である. ▌

(ε) $\bar{A}=\langle\bar{a}\rangle$, $\bar{b}\in\bar{Q}^\sharp \Longrightarrow \bar{G}=\langle\bar{a},\bar{a}^{\bar{b}}\rangle$.

[証明] (δ) により $\bar{P}=\bar{A}$ は巡回群である. $\bar{a}$ を $\bar{A}$ の生成元，$\bar{b}\in\bar{Q}^\sharp$ とする. $\bar{A}$ の $\bar{Q}$ への作用の既約性から，$[\bar{a},\bar{b}]\neq 1$ である. このとき $\langle\bar{a}\rangle\neq\langle\bar{a}^{\bar{b}}\rangle$. 実際，$\langle\bar{a}\rangle=\langle\bar{a}^{\bar{b}}\rangle$ とすると，$[\bar{a},\bar{b}]\in\langle\bar{a}\rangle\cap\bar{Q}=1$ となり矛盾である. (γ), (i) により，$\bar{P}=\bar{A}$ は $\bar{G}$ の極大部分群であるから，$\bar{G}=\langle\bar{a},\bar{a}^{\bar{b}}\rangle$ を得る. ▌

(ζ) $W=\{x\in Z(H)\mid x^p=1\}$ とおく. G の W への作用の核は H である.

[証明] 明らかに $G \triangleright W$ であるから，G は W に

$$W \ni x \longmapsto x^g = g^{-1}xg \in W \qquad (g \in G)$$

によって作用する．この作用の核を K としよう．K が位数 q の元 g を含めば，例題7.2により g は $Z(H)$ に自明な作用をする．一方，(β) により $Z(P) \subseteq Z(H)$ であるから，$g \in C_G(Z(P)) = P$ ((γ), (i) による) となり矛盾である．よって K は p 群となり，(α), (i) により $K = H$ である．▌

以下，$\bar{G} = G/H$ の W への作用を調べて最終的な矛盾を導こう．

$$W = C_W(\bar{Q}) \oplus [W, \bar{Q}], \qquad V = [W, \bar{Q}]$$

とおく．明らかに V は $\bar{G}$ 不変である．また $\bar{G}$ は V の上に忠実に作用する．実際，$\bar{K}$ を $\bar{G}$ の V への作用の核とすると，$\bar{K} \cap \bar{Q}$ は W の上に自明な作用をする．このとき (ζ) により $\bar{K} \cap \bar{Q} = 1$．よって $\bar{K}$ は p 群，(α), (i) により $\bar{K} = 1$ である．

$$A \cap H = A_0, \qquad V_0 = V \cap A = V \cap A_0$$

とおく．$\bar{P} = \bar{A}$ は巡回群であるから，

$$m(A_0) \geqq d-1$$

である．また，

$$m(V_0) = t, \qquad m(V/V_0) = r$$

とおくと，$\langle V, A_0 \rangle$ は Abel 群であることに注意して

$$\begin{aligned} d \geqq m(\langle V, A_0 \rangle) &= m(V) + m(A_0) - m(V \cap A_0) \\ &= t + r + m(A_0) - t \\ &\geqq r + d - 1 \end{aligned}$$

となるから，

$$r \leqq 1$$

を得る．(ε) のように $\bar{G} = \langle \bar{a}, \bar{a}^{\bar{b}} \rangle$ とすると，$\bar{a}, \bar{a}^{\bar{b}}$ はそれぞれ $V_0, V_0{}^b$ の上に自明な作用をするから，$\bar{G}$ は $V_0 \cap V_0{}^b$ の上に自明な作用をする．$V \subseteq [W, \bar{Q}]$ であるから，これは $V_0 \cap V_0{}^b = 1$ を意味する．ところで $r \leqq 1$ より $[V : V_0 \cap V_0{}^b] \leqq p^2$ であるから，$|V| = p^2$ となり，V は (p, p) 型の Abel 群である．ところで $\bar{G}$ の V への作用は忠実であったから，$\bar{G}$ は $GL(2, p)$ の部分群と同型で，$\bar{a}$ は $\bar{G}$ の位数 p の元である．$GL(2, p)$ の位数 p の元は，$SL(2, p)$ に含まれるから，結局 $\bar{G}$ は $SL(2, p)$ の部分群と同型である．$\bar{Q}$ は基本 Abel 群であったから，問7.18により $|\bar{Q}| = q$ となる．したがって $\bar{G}$ は位数 pq の非可換群で S_q 部分群は $\bar{G}$ の正

規部分群である．このとき補題7.24により $p=2$ となり矛盾である．これで定理7.15の証明は完成された．▌

e）Frobenius 群 II

ここでは最初に，この章の目標の一つであった“Frobenius 群の Frobenius 核の巾零性”の証明を与えよう．前にも言及したように，証明の鍵となるのは Thompson の定理7.15である．

定理 7.16(Thompson)　Frobenius 群の Frobenius 核は巾零群である．

証明　G を最小位数の反例とする．N を G の Frobenius 核とする．仮定により N は巾零ではない．H を Frobenius 群 (G,N) の Frobenius 補群とする．このとき，補題7.17により H は奇数位数である．さらに定理7.10と例題7.6により H は可解群である．問7.17と G の最小性から，

(7.48)　N の H 不変な真の部分群は，巾零群，

(7.49)　$G \triangleright N_0$，$1 \neq N_0 \subseteqq N \Longrightarrow N/N_0$ は巾零群

であることがわかる．以下，(G,N) の性質を段階に分けて調べ，矛盾を導こう．

(α)　$Z(N)=1$.

[証明]　$(G/Z(N), N/Z(N))$ は，Frobenius 群だから，$Z(N)\neq 1$ ならば，(7.49)により $N/Z(N)$ は巾零となる．このとき，N も巾零となり矛盾である．▌

(β)　$|N|$ を割る或る素数 p に対して，N の S_p 部分群は G の正規部分群である．

[証明]　$|N|$ を割る或る素数 p に対して $N \triangleright J(P)$，$P \in \mathrm{Syl}_p(N)$ と仮定する．このとき，$J(P)$ は H 不変である．実際，$H \ni h$ とすると，$J(P)^h=J(P^h)=J(P^n)=J(P)^n=J(P)$ $(\exists n \in N)$ である．したがって $G \triangleright J(P)$ となるから，(7.49)により $N/J(P)$ は巾零である．このとき，明らかに $N \triangleright P$，よって $G \triangleright P$ となる．したがって $|N|$ を割るすべての素数 p に対して $N_N(J(P)) \neq N$，$P \in \mathrm{Syl}_p(N)$ としてよい．定理7.6により P は H 不変にとれる．このとき，$N_N(J(P))$ も H 不変となり，(7.48)により $N_N(J(P))$ は巾零とくに p 巾零である．また(α)により $C_N(Z(P)) \neq N$ であるから，再び(7.48)により $C_N(Z(P))$ も p 巾零である．したがって定理7.15により，p が奇素数のとき，N は p 巾零である．このとき，問7.23により，N の S_2 部分群は N の正規部分群，したがって G の正規部分群である．▌

(γ) (β)により $G \triangleright P$, $P \in \mathrm{Syl}_p(N)$ なる素数 p が存在する．$C = C_G(Z(P))$ とおくと，$G \triangleright C$ は明らかである．またFrobenius核の定義(7.24)により $C \subseteqq N$ であるが，(α)により $C \subsetneqq N$ である．よって(7.49)により G/C は N/C を Frobenius核とするFrobenius群で，$\bar{H} = HC/C$ がそのFrobenius補群である．$V = Z(P)$ とおく．このとき，G/C の V への作用は，補題7.19の仮定を満たすから，$C_V(\bar{H}) \neq 1$ または $C_V(\bar{N}) \neq 1$ である．$C_V(\bar{N}) \neq 1$ ならば，$1 \neq C_V(\bar{N}) = C_V(N) \subseteqq Z(N)$ となるから(α)に反する．よって，$C_V(\bar{H}) \neq 1$ である．このとき，$C_V(\bar{H}) = C_V(H)$ より $C_V(H) \neq 1$．一方，$H \cdot V = H \cdot Z(P)$ は(7.48)により $Z(P)$ をFrobenius核とするFrobenius群であるから，(7.30)により $C_V(H) = 1$ となり矛盾である．▌

系 固定点のない素数位数の自己同型をもつ有限群は巾零群である．

証明 N を有限群，σ を N の素数位数の自己同型で，N の上に(単位元以外の)固定点をもたないようなものとする．このとき，半直積 $\langle\sigma\rangle \cdot N$ は，補題7.16によりFrobenius群で N がそのFrobenius核である．よって定理7.16により N は巾零群である．▌

上で証明した"Frobenius核の巾零性"は，"奇数位数の群の可解性"とともに有限群論の古典的難問題であった．これらの問題は，1960年を境として相次いで解決されたのであるが，それは主としてThompsonの天才に負う所が大きい．定理7.16がThompsonにより証明されたのは1959年であるが，その原証明は著しく難解なものであった[1)]．それが，この基礎数学講座で取り上げられるようになったというのも，近年(1960年以降)の有限群論の一つの進歩を示すといえるであろう．一方，"奇数位数の群の可解性"については，その証明は極めて難解なものであって，その全証明を書物で取り上げることは(たとえそれが専門家向けのものであっても)，いまだに不可能であろう．しかし，その証明の重要な一部については，そこで使われた考え方が発展整備され，その後の有限単純群論にとって大切な役割を果たすようになっている．本講でもつぎの§7.4で，それらの主な事柄を解説する．——

さて，Frobenius群に話を戻し，Frobenius核の一意性とFrobenius群の二,

1) 定理7.16の証明というよりは，その鍵となる定理7.15(に相当する或る定理)の証明が難しかった．

三の大切な性質にふれて，この項を終ることにしよう．

定理 7.17 (i) Frobenius 群の Frobenius 核は一意的に定まる．

(ii) 二つの Frobenius 補群は，互いに共役である．

証明 (i) N_1, N_2 を G の Frobenius 核すなわち(7.24)を満たす G の正規部分群としよう．$N_1 \neq N_2$ と仮定して矛盾を導く．このとき (7.24) から明らかなように，$N_1 \cap N_2$ も (7.24) を満たすから，補題 7.14 により，$|N_1|$ を割り $|N_1 \cap N_2|$ を割らない素数 p が存在する．$P \in \mathrm{Syl}_p(N_1)$ とすれば，定理 7.16 により $[P, N_1 \cap N_2]=1$．これは $N_1 \cap N_2$ が (7.24) を満たすことに反する．

(ii) H を Frobenius 群 (G, N) の Frobenius 補群としよう．定理 7.16 により，N は巾零群とくに可解群だから，Schur-Zassenhaus の定理から (ii) は直ちに得られる．(補題 7.14 により H と N の位数は互いに素であることに注意.) しかし，H または N の可解性は定理 7.16 を用いなくても補題 7.17，定理 7.10，例題 7.6 からも得られる(定理 7.16 の証明の最初の部分を参照)．▌

定理 7.18 Frobenius 群の Frobenius 補群の中心は単位群ではない．

証明 H は Frobenius 群 G の Frobenius 補群，p は $|H|$ を割る最小の素数とする．x を H の位数 p の元とするとき，$x \in Z(H)$ を示そう．$p=2$ のとき，これは補題 7.17 からわかる．よって p を奇素数したがって H は奇数位数としよう．このとき，定理 7.10 と例題 7.6 により H は可解群である．$F(H)$ を H の Fitting 部分群 (=H の最大の巾零正規部分群) とするとき，$x \in F(H)$ をいえばよい．実際，$F(H)$ は定理 7.10 により巡回群だから，$x \in F(H)$ のとき $\langle x \rangle \lhd H$ となり，p が $|H|$ を割る最小の素数であるから，H の元の $\langle x \rangle$ への作用を考えて，$[H, x]=1$ を得る．したがって $x \notin F(H)$ として矛盾を導こう．y を $F(H)$ の素数位数 q の元とすると，$\langle y \rangle \lhd H$ であるから，$\langle x, y \rangle$ は位数 pq の H の部分群である．よって定理 7.9 により $\langle x, y \rangle$ は巡回群である．したがって x は $F(H)$ の素数位数の任意の元と可換である．このとき例題 7.2 により，$[x, F(H)]=1$．したがって定理 5.6 により，$x \in C_G(F(H)) \subseteq F(H)$ となり矛盾である．▌

問 7.26 H を Frobenius 群の Frobenius 補群とする．H が奇数位数ならば，$|H|$ を割る素数は $|F(H)|$ を割ることを示せ．[ヒント] 定理 7.18 の証明をよく見よ！

§7.4 Glauberman の ZJ 定理

本節で解説するすべての概念や結果は，“奇数位数の群の可解性” の証明の中で使われた考え方を発展整備したものであり，現在の有限単純群論で基本的な役割を果たしているものである．したがって，その内容は，少し専門的な感が無きにしもあらずであるが，最近の有限群論で使われている基本的な事柄がどのようなものであるかを，多少とも理解して頂ければ幸いである．有限群の p 束縛性 (p-constraint)，p 安定性 (p-stability)，Glauberman の ZJ 定理などがその主なものである．最後に $p=2$ に対する信号関手定理の Bender による証明を紹介する．

a) p 束縛群

G を有限群，p を素数とする．§7.2, d) におけるように，位数が p と素な群を p' 群という．つぎの (7.50), (7.51) は容易に証明される：

(7.50)　P_1, P_2 が G の正規 p 部分群ならば，P_1P_2 もそうである，

(7.51)　N_1, N_2 が G の正規 p' 部分群ならば，N_1N_2 もそうである．

問 7.27　(7.50), (7.51) を確かめよ．——

(7.50) により G の正規 p 部分群で極大なものがただ一つ存在する．それを $O_p(G)$ で表わそう：

$$O_p(G) = G \text{ の最大の正規 } p \text{ 部分群}.$$

同様に (7.51) により G の正規 p' 部分群で極大なものがただ一つ存在する．それを $O_{p'}(G)$ で表わす：

$$O_{p'}(G) = G \text{ の最大の正規 } p' \text{ 部分群}.$$

問 7.28　H を有限群 G の部分群とする．つぎの (i), (ii) を示せ：

(i)　$O_{p'}(G) \cap H \subseteq O_{p'}(H)$,　$O_p(G) \cap H \subseteq O_p(H)$,

(ii)　$G \triangleright H \Longrightarrow O_{p'}(G) \cap H = O_{p'}(H)$,　$O_p(G) \cap H = O_p(H)$．——

ここで第5章§5.3で定義された $F^*(G)$ の定義を思い起そう：

$$F^*(G) = F(G)E(G),$$
$$F(G) = G \text{ の最大の巾零正規部分群},$$
$$E(G) = G \text{ の最大の半単純正規部分群}.$$

$O_p(G)$ は $F(G)$ の S_p 部分群にほかならない．$F^*(G)$ のもっとも大切な性質は，

(7.52)　　$C_G(F^*(G)) \subseteq F^*(G)$　　(定理 5.5)

である．

問 7.29　$G \triangleright H$ のとき，$E(H) \subseteq E(G)$，$F(H) \subseteq F(G)$．

問 7.30 $F^*(G)$ を p 群とする．$F^*(G)=P$，$\bar{P}=P/\Phi(P)$ とおく．G の $\bar{P}$ への(共役による)作用の核は P であることを示せ．[ヒント] 補題 7.12 の (i) と (7.52) の応用．——

つぎの補題は補題 7.12 の (iv) の変形であるが，'Thompson の $A\otimes B$ 補題' とよばれているものである．

補題 7.25 (Thompson) p' 群 A と p 群 B の直積 $A\otimes B$ が p 群 P に作用しているとする．このとき，

$$[C_P(B), A]=1 \Longrightarrow [P, A]=1.$$

証明 $A\otimes B$ と P の半直積 $G=(A\otimes B)\cdot P$ を考える．G の部分群 BP を X とおく：$X=BP$．$G=AX\triangleright X$ であるから A は X に素な作用をする．また $Y=BC_P(B)$ とおくと，$C_X(Y)\subseteqq Y$ である．実際，$C_X(Y)=C_{BP}(BC_P(B))\subseteqq C_{BP}(B)=Z(B)C_P(B)\subseteqq BC_P(B)=Y$．補題の仮定により $[A, Y]=1$ だから，補題 7.12 の (iv) により $[A, X]=1$，とくに $[A, P]=1$ である．▌

G の部分群 L が，単位群でない或る p 部分群の正規化群であるとき，L を G の **p 局所部分群**という：

$$L=p\text{ 局所部分群} \Longleftrightarrow L=N_G(H) \qquad (H=p\text{ 部分群}\neq 1).$$

補題 7.26 L を G の p 局所部分群とするとき，

(i) $[O_{p'}(L), O_p(G)]=1$,

(ii) $[E(L), O_p(G)]=1$.

証明 $L=N_G(H)$，$H=p$ 部分群$\neq 1$ とする．$[O_{p'}(L), H]\subseteqq O_{p'}(L)\cap H=1$ であるから，$O_{p'}(L)H=O_{p'}(L)\otimes H$．$P=O_p(G)$ とおき，$O_{p'}(L)H$ の P への作用を考える．$O_{p'}(L), C_P(H)\lhd L$ であるから，$[C_P(H), O_{p'}(L)]\subseteqq C_P(H)\cap O_{p'}(L)=1$．よって，$A=O_{p'}(L)$，$B=H$，$P=O_p(G)$ として，上の $A\otimes B$ 補題 7.25 を適用すれば，$[O_{p'}(L), O_p(G)]=1$ を得る．よって (i) が示された．(ii) を示すには，$E(L)$ は位数が p と素な元で生成されるから，x をそのような $E(L)$ の元とするとき，$[x, P]=1$ をいえば十分である．$[\langle x\rangle, H]\subseteqq[E(L), H]\subseteqq[E(L), O_p(L)]=1$ より，$\langle x\rangle H=\langle x\rangle\otimes H$．また，$[C_P(H), \langle x\rangle]\subseteqq[O_P(L), \langle x\rangle]=1$．よって $A=\langle x\rangle$，$B=H$，$P=O_p(G)$ として，$A\otimes B$ 補題 7.25 を用いて，$[P, \langle x\rangle]=1$ を得る．▌

定理 7.19 L を G の p 局所部分群とする．$F^*(G)$ が p 群ならば，$F^*(L)$ も

p 群である.

証明 $F^*(G)=O_p(G)$ である. このとき, (7.52) により $C_G(O_p(G))\subseteqq O_p(G)$. 一方, 補題7.26 により $O_{p'}(L)\subseteqq C_G(O_p(G))$. よって $O_{p'}(L)\subseteqq O_p(G)$ すなわち $O_{p'}(L)=1$ を得る. とくに $F(L)=O_p(L)$ である. 再び補題7.26 により $E(L)\subseteqq C_G(O_p(G))\subseteqq O_p(G)$. よって $E(L)=1$. したがって $F^*(L)=F(L)E(L)=F(L)=O_p(L)$ である. ▌

有限群 G が

$$F^*(G/O_{p'}(G))=p\ \text{群}$$

なる条件を満たすとき, G を **p 束縛群** (p-constrained group) という. $\bar{G}=G/O_{p'}(G)$ とおくとき,

$$G=p\ \text{束縛} \Leftrightarrow C_{\bar{G}}(O_p(\bar{G}))\subseteqq O_p(\bar{G})$$

である. 実際, $\Longrightarrow$ は (7.52) から明らかであり, $\Longleftarrow$ は $E(\bar{G})\subseteqq C_{\bar{G}}(O_p(\bar{G}))\subseteqq O_p(\bar{G})$ より $E(\bar{G})=1$ となることからわかる.

例 7.3 p 束縛群のもっとも簡単な例は, 可解群である. すなわち, 可解群は任意の素数 p に対して p 束縛である. 実際, G を可解群, $\bar{G}=G/O_{p'}(G)$ とおくと, $\bar{G}$ も可解群だから, $E(\bar{G})=1$ となり, $O_{p'}(\bar{G})=1$ に注意すれば $F^*(\bar{G})=F(\bar{G})E(\bar{G})=F(\bar{G})=O_p(\bar{G})$ を得る.

問 7.31 p 束縛群の正規部分群は p 束縛群である.

問 7.32 H を G の p 部分群 $(\neq 1)$ とする. つぎの (i), (ii), (iii) を示せ:

(i) $O_{p'}(N_G(H))=O_{p'}(C_G(H))$,

(ii) $E(N_G(H))=E(C_G(H))$,

(iii) $N_G(H)$ が p 束縛 $\Leftrightarrow$ $C_G(H)$ が p 束縛. ——

ここで p 束縛群の大切な例であり, また可解群の概念の一般化でもある p 可解群について説明しよう. 有限群 G の組成列の各組成因子が p 群または p' 群であるとき, G を **p 可解群**という. G が

$$G=G_0\rhd G_1\rhd\cdots\rhd G_{n-1}\rhd G_n=1,$$
$$G_{i-1}/G_i\quad \text{は}\quad p\ \text{群 または}\ p'\ \text{群}$$

なる正規列をもてば, Jordan-Hölder の定理により G は p 可解群である. このことからつぎのことが容易にわかる:

(7.53) p 可解群の部分群, 剰余群は p 可解群である,

(7.54) 有限群 G が可解群であるためには，G の位数を割る任意の素数 p に対して p 可解群であることが必要十分である．

問 7.33 (7.53), (7.54) を証明せよ．

補題 7.27 半単純 p 可解群は p' 群である．

証明 G を半単純 p 可解群とする．$G/Z(G)$ は非可換単純群の直積であるから，$G/Z(G)$ は p' 群である．$p \mid |Z(G)|$ と仮定して矛盾を導こう．$P \in \mathrm{Syl}_p(Z(G))$ とすると，$P \lhd G$ である．$G/Z(G)$ は p' 群だから $P \in \mathrm{Syl}_p(G)$ である．よって G/P に Schur-Zassenhaus の定理を適用して，その補群を H とすると，$G=HP$, $H \cap P=1$. しかるに，$P \subseteqq Z(G)$ であるから $G=HP=H \otimes P$ となる．両辺の交換子を作ると $G' \subseteqq H' \subseteqq H$ となり，$G=G'$ に矛盾する．▌

定理 7.20 p 可解群は p 束縛群である．とくに G が $O_{p'}(G)=1$ なる p 可解群ならば $C_G(O_p(G)) \subseteqq O_p(G)$ である．

証明 G を p 可解群とする．$\bar{G}=G/O_{p'}(G)$ とすると，(7.53), (7.54) により $\bar{G}$, $E(\bar{G})$ も p 可解群である．補題 7.27 により $E(\bar{G})$ は p' 群であるが，$O_{p'}(\bar{G})=1$ であるから，$E(\bar{G})=1$ を得る．したがって $F^*(\bar{G})=O_p(\bar{G})$ となり，G は p 束縛である．定理の後半は，$F^*(G)=O_p(G)$ と (7.52) から得られる．▌

p 束縛群の他の例については，後の例 7.4, 例題 7.8 を見よ．つぎの三つの補題は，有限群の p 局所部分群と p 束縛性についての基本事項である．

補題 7.28 G を p 束縛群，L を G の p 局所部分群とする．このとき，つぎの (i), (ii) が成り立つ：

(i) $O_{p'}(L) \subseteqq O_{p'}(G)$, $E(L) \subseteqq O_{p'}(G)$,

(ii) L も p 束縛群である．

証明 $L=N_G(H)$, $H=p$ 部分群$\neq 1$ とする．$\bar{G}=G/O_{p'}(G)$ とおくと，補題 7.10 により $\bar{L}=N_{\bar{G}}(\bar{H})$ すなわち $\bar{L}$ は $\bar{G}$ の p 局所部分群である．よって定理 7.19 により $F^*(\bar{L})$ も p 群．とくに $O_{p'}(\bar{L})=1$, $E(\bar{L})=1$ である．ところで

$$\bar{L} = LO_{p'}(G)/O_{p'}(G) \simeq L/O_{p'}(G) \cap L \tag{7.55}$$

であるから，$O_{p'}(\bar{L})=1$ より $O_{p'}(L)=O_{p'}(G) \cap L \subseteqq O_{p'}(G)$, また $\overline{E(L)} \subseteqq E(\bar{L})=1$ より $E(L) \subseteqq O_{p'}(G)$ を得る．さらに $O_{p'}(L)=O_{p'}(G) \cap L$ と (7.55) により $\bar{L} \simeq L/O_{p'}(L)$. したがって $F^*(\bar{L}) \simeq F^*(L/O_{p'}(L))$ は p 群である．▌

つぎの例題は，信号関手が現われるもっとも典型的な場合を示すものである．

例題 7.7 A を G の可換 p 部分群とする．

$$A^{\sharp} \ni a \Longrightarrow C_G(a) = p \text{ 束縛} \tag{7.56}$$

と仮定する．このとき

$$O_{p'}(C_G(a)) \cap C_G(b) \subseteqq O_{p'}(C_G(b)) \qquad (\forall a, b \in A^{\sharp})$$

である．すなわち，仮定 (7.56) のもとに，$A^{\sharp} \ni a \mapsto O_{p'}(C_G(a))$ は，G の A 信号関手である．

［証明］ $A^{\sharp} \ni a, b$ とする．$X = C_G(b)$ とおくと，$a \in X$ である．仮定 (7.56) により X は p 束縛だから，問 7.32 の (iii) と補題 7.28 の (i) により

$$O_{p'}(C_X(a)) = O_{p'}(N_X(\langle a \rangle)) \subseteqq O_{p'}(X)$$

である．$O_{p'}(C_G(a)) \cap X$ は，$C_X(a)$ の正規 p' 部分群であるから

$$O_{p'}(C_G(a)) \cap C_G(b) \subseteqq O_{p'}(C_X(a)) \subseteqq O_{p'}(X) = O_{p'}(C_G(b))$$

を得る．▌

補題 7.29 U, V を G の単位群でない p 部分群で $U \supseteqq V$ とする．このとき，

$$N_G(V) \text{ が } p \text{ 束縛} \Longrightarrow N_G(U) \text{ も } p \text{ 束縛}.$$

証明 p 群の性質により

$$U = U_0 \triangleright U_1 \triangleright \cdots \triangleright U_{n-1} \triangleright U_n = V$$

なる部分群の列 $U_0, U_1, \cdots, U_n$ が作れるから，始めから $U \triangleright V$ と仮定してよい．このとき，$N_G(V) \cap N_G(U)$ は p 束縛群 $N_G(V)$ の p 局所部分群だから，補題 7.28 により p 束縛である．よって

$$N_G(U) \cap N_G(V) \triangleright C_G(U) \cap C_G(V) = C_G(U)$$

に注意すれば，問 7.32 の (iii) により $C_G(U)$ も p 束縛である．再び問 7.32 の (iii) を用いて $N_G(U)$ も p 束縛となる．▌

補題 7.30 (Gorenstein) つぎの 3 条件は同値である：

(i) G のすべての p 局所部分群が p 束縛，

(ii) G のすべての極大 p 局所部分群が p 束縛，

(iii) G の位数 p の任意の元の中心化群が p 束縛．

証明 (i) $\Longrightarrow$ (ii) は自明である．(ii) $\Longrightarrow$ (iii) を示そう．x を G の位数 p の元とする．$N_G(\langle x \rangle)$ を含む極大 p 局所部分群を L とすると，(ii) により L は p 束縛．$N_G(\langle x \rangle)$ は L の p 局所部分群だから，補題 7.28 により $N_G(\langle x \rangle)$ も p 束縛となる．問 7.32 の (iii) により $C_G(x)$ も p 束縛である．最後に (iii) $\Longrightarrow$ (i) を

示そう．H を G の p 部分群 $(\neq 1)$ とする．x を H の位数 p の元とすると，(iii) により $C_G(x)$ は p 束縛．よって問 7.32 の (iii) により $N_G(\langle x\rangle)$ も p 束縛である．$U=H$, $V=\langle x\rangle$ として補題 7.29 を適用すれば，$N_G(H)$ も p 束縛となる．∎

例 7.4 $G=GL(n,q)$ ($q=p^e$, p 素数) とする．G の対角成分が 1 の上半三角行列全体の集合を $T(n,q)$ とする：

$$T(n,q)=\left\{\begin{bmatrix}1 & & & *\\ & 1 & & \\ & & \ddots & \\ 0 & & & 1\end{bmatrix}\in GL(n,q)\right\}.$$

$T(n,q)$ は G の S_p 部分群である．$1\leqq k\leqq n-1$ なる任意の整数 k に対して

$$A_k=\left\{\begin{bmatrix}E_k & *\\ 0 & E_{n-k}\end{bmatrix}\in T(n,q)\right\}$$

とおく．行列の計算により

$$C_G(A_k)=A_k\otimes Z(G)$$

が容易にわかる．ここで $Z(G)$ は G のスカラー行列全体の集合であることに注意．$|Z(G)|=q-1$ であるから，$Z(G)$ は p' 群である．したがって $C_G(A_k)$ は p 束縛である．問 7.32 の (iii) により $N_G(A_k)$ も p 束縛である．$N_G(A_k)$ を計算すると，

$$N_G(A_k)=\left\{\begin{bmatrix}X & *\\ 0 & Y\end{bmatrix}\middle| X\in GL(k,q),\ Y\in GL(n-k,q)\right\}$$

となる．$1\leqq l\leqq n/2$ なる任意の整数 l に対して

$$x_l=\begin{bmatrix}E_l & 0 & E_l\\ 0 & E_{n-2l} & 0\\ 0 & 0 & E_l\end{bmatrix}$$

とおくと，x_l は G の位数 p の元である．$C_G(x_l)$ を計算すると，

$$C_G(x_l)=\left\{\begin{bmatrix}U & * & *\\ 0 & V & *\\ 0 & 0 & U\end{bmatrix}\middle| U\in GL(l,q),\ V\in GL(n-2l,q)\right\}$$

である．とくに $C_G(x_l)\subseteqq N_G(A_l)$ がわかる．よって補題 7.28 により $C_G(x_l)$ は p 束縛となる．ところで

(7.57) $p=2$ のとき，G の位数 2 の元は或る x_l と共役

であることが証明される(Jordan 標準形を考えればよい). したがって補題7.30により

(7.58) $GL(n, 2^e)$ の任意の2局所部分群は2束縛

であることがわかる. 奇素数 p に対しても (7.58) に対応する命題が成立するのであるが, このときは (7.57) に相当することが必ずしも成立しないので計算は複雑になる. 興味のある読者は, 奇素数 p に対して (7.58) の証明を試みられたい. なお標数 p の有限体の上の Chevalley 群, Steinberg 群などいわゆる Lie 型の群に対して (7.58) に対応する命題が成り立つことが知られている.

問 7.34 (7.57) を確かめよ.

問 7.35 $A_k^\sharp \ni \forall x$ に対して $C_G(x)$ は p 束縛であることを示せ (p は任意の素数).

例題 7.8 G を有限群, $\mathrm{Syl}_p(G) \ni P$ とする. Q を

$$P \rhd Q, \quad C_P(Q) \subseteqq Q \tag{7.59}$$

なる性質をもつ P の部分群とする. このとき

(i) $C_G(Q) = Z(Q) \otimes O_{p'}(C_G(Q))$,

(ii) $N_G(Q)$ は p 束縛である.

[証明] (7.59) により, $\mathrm{Syl}_p(N_G(Q)) \ni P$ である. $N_G(Q) \rhd C_G(Q)$ であるから, $P \cap C_G(Q) = C_P(Q) = Z(Q)$ は $C_G(Q)$ の S_p 部分群である. 明らかに $C_G(Q) \rhd Z(Q)$ であるから, 剰余群 $G_G(Q)/Z(Q)$ に Schur-Zassenhaus の定理を適用して, その補群を H とすると, $C_G(Q) = HZ(Q)$, $H \cap Z(Q) = 1$. しかるに $[H, Z(Q)] = 1$ であるから

$$C_G(Q) = H \otimes Z(Q), \qquad H = O_{p'}(C_G(Q))$$

となる. とくに $C_G(Q)$ は p 束縛である. よって問 7.32 の (iii) により $N_G(Q)$ も p 束縛である. ▌

問 7.36 $G = GL(n, q)$, $T(n, q)$, A_k を例 7.4 のようにとると, $T(n, q)$, A_k は (7.59) を満たす.

例題 7.9 p 群の極大可換正規部分群は (7.59) を満たす.

[証明] P を p 群, A を P の極大可換正規部分群とする. $C_P(A) = A$ を示さなければならない. 明らかに $C_P(A) \supseteqq A$ だから $C_P(A) \supsetneqq A$ と仮定して矛盾を導こう. $C = C_P(A)$, $\bar{P} = P/A$ とおく. $\bar{P} \rhd \bar{C} \neq 1$ であるから, $\bar{C}$ は $\bar{P}$ の位数 p の正

規部分群 $\bar{D}=D/A$ を含む．D/A は巡回群で $Z(D)\supseteqq A$ であるから，D は可換部分群である．$P\triangleright D$ は明らかであるから，これは A の極大性に反する．∎

p 群 P の極大可換正規部分群の集合を，$\mathcal{SCN}(P)$ と書く．G を有限群，$\mathrm{Syl}_p(G)\ni P$，$\mathcal{SCN}(P)\ni A$ $(m(A)\geqq 2)$ とする．A が

(7.60) $\qquad A^{\sharp}$ の任意の元 a に対して $C_G(a)$ は p 束縛

なる条件を満たすとする．このとき例題 7.7 により

$$\theta(C_G(a))=O_{p'}(C_G(a)) \qquad (\forall a\in A^{\sharp})$$

とおくと，θ は A 信号関手である．以下で，このような A 信号関手に対しては，任意の A 不変 p' 部分群は θ 部分群であることを示そう．(一般の信号関手に対しては，θ 部分群は定義により A 不変 p' 部分群であるが，逆は必ずしも成立しない．)

補題 7.31 G を p 束縛群，$\mathrm{Syl}_p(G)\ni P$，$P\triangleright Q$ とする．X を G の Q 不変 p' 部分群とするとき，

(i) $[Q,X]\subseteqq O_{p'}(G)$,

(ii) $C_P(Q)\subseteqq Q$ ならば $X\subseteqq O_{p'}(G)$.

証明 (i) 剰余群 $\bar{G}=G/O_{p'}(G)$ にうつって，$[\bar{Q},\bar{X}]=1$ をいえばよいから，始めから $O_{p'}(G)=1$ としてよい．$R=O_p(G)$ とおく．$P\triangleright Q,R$ より $[Q,R]\subseteqq Q\cap R$. よって

(7.61) $$[Q,R,X]\subseteqq[Q\cap R,X]\subseteqq X\cap R=1.$$

$\bar{R}=R/[Q,R]$ とおく．Q,X は $\bar{R}$ に作用し，Q は $\bar{R}$ に自明な作用をするから，

$$[Q,\bar{R},X]=1, \qquad [\bar{R},X,Q]\subseteqq[\bar{R},Q]=1$$

である．よって 3 部分群補題 5.8 により

(7.62) $$[X,Q,\bar{R}]=1.$$

(7.61), (7.62) により $[X,Q]$ は $R/[R,Q]$ と $[R,Q]$ に自明な作用をする．よって補題 7.12 の (ii) により $[X,Q]$ は R に自明な作用をする．すなわち $[X,Q]\subseteqq C_G(R)\subseteqq R$ となり，$[X,Q]=1$ を得る．

(ii) 例題 7.8 の (i) により $C_G(Q)=Z(Q)\otimes O_{p'}(C_G(Q))$ であるから，$C_X(Q)\subseteqq O_{p'}(C_G(Q))$ である．よって補題 7.28 により

$$C_X(Q)\subseteqq O_{p'}(C_G(Q))\subseteqq O_{p'}(G).$$

一方，定理 7.5 の系により $X=[Q,X]C_X(Q)$. (i) により $[Q,X]\subseteqq O_{p'}(G)$ で

あるから，$X \subseteqq O_{p'}(G)$ を得る．∎

定理 7.21　$\mathrm{Syl}_p(G) \ni P$, $\mathscr{SCN}(P) \ni A$, $m(A) \geqq 2$ とする．さらに A は(7.60)を満たすと仮定する．X が A 不変 p' 部分群ならば，$C_X(a) \subseteqq O_{p'}(C_G(a))$ $(\forall a \in A^\sharp)$ である．すなわち $\theta(C_G(a)) = O_{p'}(C_G(a))$ なる A 信号関手に対しては，任意の A 不変 p' 部分群は θ 部分群である．

証明　p 群の性質により，$P \triangleright B$, $B \subseteqq A$ なる (p, p) 型の部分群 B が存在する．このとき $[P : C_P(B)] \leqq p$ である．B の位数 p の部分群の全体を $B_0, B_1, \cdots, B_p$ として，$B_i = \langle b_i \rangle$ とおく．$Z(P) \cap B \neq 1$ だから，$b_0 \in Z(P)$ としておく．まず

$$C_X(b_i) \subseteqq O_{p'}(C_G(b_i)) \qquad (0 \leqq i \leqq p) \tag{7.63}$$

を示そう．$i=0$ に対しては，$\mathrm{Syl}_p(C_G(b_0)) \ni P$ であるから，補題 7.31 の (ii) の G, P, Q, X としてそれぞれ $C_G(b_0), P, A, C_X(b_0)$ をとれば，$C_X(b_0) \subseteqq O_{p'}(C_G(b_0))$ を得る．このとき，例題 7.7 により

$$C_X(B) \subseteqq O_{p'}(C_G(b_0)) \cap C_G(b_i) \subseteqq O_{p'}(C_G(b_i)) \tag{7.64}$$

である．つぎに $i>0$ とし，$X_i = [C_X(b_i), B]$ とおく．$\mathrm{Syl}_p(C_G(b_i)) \ni P_i \supseteqq P^* = C_P(B)$ とすると，$[P_i : P^*] \leqq p$ であるから，$P_i \triangleright Z(P^*) \supseteqq B$ である．X_i は A 不変で，$A \supseteqq Z(P^*)$ (A の極大性!) だから，X_i は $Z(P^*)$ 不変である．また定理 7.5 の系により $[X_i, B] = X_i$ であるから，$X_i = [X_i, B] \subseteqq [X_i, Z(P^*)] \subseteqq X_i$. よって $[X_i, Z(P^*)] = X_i$ を得る．補題 7.31 の (i) の G, P, Q, X としてそれぞれ $C_G(b_i)$, $P_i, Z(P^*), X_i$ をとれば，

$$X_i \subseteqq O_{p'}(C_G(b_i)) \tag{7.65}$$

である．一方，定理 7.5 の系により

$$C_X(b_i) = [C_X(b_i), B](C_X(b_i) \cap C_X(B)) = [C_X(b_i), B]C_X(B)$$

であるから，(7.64), (7.65) により $C_X(b_i) \subseteqq O_{p'}(C_G(b_i))$ すなわち (7.63) を得る．$A^\sharp \ni a$ としよう．このとき，定理 7.7 により

$$C_X(a) = \langle C_X(a, b_i) \mid 0 \leqq i \leqq p \rangle$$

である．(7.63) と例題 7.7 により

$$C_X(a, b_i) \subseteqq O_{p'}(C_G(b_i)) \cap C_G(a) \subseteqq O_{p'}(C_G(a)).$$

したがって $C_X(a) \subseteqq O_{p'}(C_G(a))$ である．∎

定理 7.22 (Thompson の可移性定理)　$\mathrm{Syl}_p(G) \ni P$, $\mathscr{SCN}(P) \ni A$, $m(A) \geqq 3$ とする．さらに A は (7.60) を満たすとする．q を p と異なる素数，$\mathscr{U}(A ; q)$ を

A 不変 q 部分群全体の集合とするとき，$C_G(A)$ は，$\mathit{U}(A;q)$ の極大元の上に可移に作用する．

証明 例題 7.7 により $\theta(C_G(a))=O_{p'}(C_G(a))$ は G の A 信号関手である．また $C_G(A)=A\otimes D$, $D=p'$ 群，とすると，$\theta(C_G(A))=D$ である．定理 7.21 により $\mathit{U}_\theta{}^*(A;q)$ は $\mathit{U}(A;q)$ の極大元全体にほかならない．このとき，この定理は定理 7.8 のいいかえにすぎない．▌

この定理は，“奇数位数の群の可解性”の証明の中で極小単純群(真の部分群が可解群であるような単純群)に対して Thompson が証明したものである．それをここで述べた形に一般化したのは Gorenstein である．さらにこの定理のいろいろな応用を通じて信号関手の概念が得られ，有限単純群論への応用が一層広くなった．このような概念を明確に捉え得たことは，近年の有限群論の進歩を示しているといえよう．

問 7.37 $\mathrm{Syl}_p(G)\ni P$, $\mathscr{SCN}(P)\ni A$, A は (7.60) を満たすとする．このとき，A を含む G の p 局所部分群は p 束縛であることを示せ．[ヒント] $L=N_G(H)\supseteq A$ のとき，$A\cap H\neq 1$ をまず示して補題 7.29 を用いる．——

G, A は定理 7.22 の仮定を満たすとしよう．このとき，(信号関手に関する)可移性定理 7.8 のすぐ後の注意で述べたように

$$G \text{ の } A \text{ 不変 } p' \text{ 部分群で最大のものの存在}$$

を期待することができる．事実，$O_{p'}(C_G(a))$ $(\forall a\in A^\sharp)$ が可解群ならば，定理 7.21 と信号関手定理により，これは真である．ところで，$\theta(C_G(a))=O_{p'}(C_G(a))$ なる特別な信号関手に対しては，より強く(もちろん定理 7.22 の仮定のもとに)

$$O_{p'}(C_G(a))\subseteq O_{p'}(G) \qquad (\forall a\in A^\sharp)$$

であることも期待できないわけではない(G 自身 p 束縛群ならば，補題 7.28 によりこれは真であることに注意)．事実，$p=2$ ならばこのことは真であることが，Gorenstein-Walter により証明されていて，それはいわゆる非成分型の有限群の基本性質の一つである．ここで，偶数位数の有限群 G は，位数 2 の或る元 t の中心化群 $C_G(t)$ が 2 束縛でないとき，**成分型の群**とよばれる．したがって，

$$G = \text{非成分型} \iff C_G(t) = 2\text{ 束縛} \qquad (t \text{ は } G \text{ の任意の位数 } 2 \text{ の元})$$

である．成分型，非成分型の有限群の典型的な例は，例 7.4 からも推察されるように，

非成分型……標数2の有限体上の Lie 型の群,

成 分 型……奇標数の有限体上の Lie 型の群

である．ただし，後者において階数(次元)の小さいものは非成分型であることもある．この項で説明してきたことは，$p=2$ に対しては非成分型の群に関係したことであるが，近年(1974年以降) Aschbacher を中心として成分型の群について目覚しい進展がなされていて，近いうちに一段落つくのではないか(有限単純群の分類が非成分型のそれに帰着されるのではないか)という形勢になっている．これについては，興味のある読者は，雑誌"数学"27巻(1975年4月)の鈴木通夫氏の論説を参照されたい．

b) p 安定的作用

G を有限群，$P\in \mathrm{Syl}_p(G)$ としよう．

(＊) $F^*(G)$ が p 群 すなわち $F^*(G)=O_p(G)$

であるとき，明らかに $F^*(G)\subseteqq P$ である．それでは，$F^*(G)$ は P のどんな部分群であろうか．あるいは，P のどんな部分群が G の正規部分群であろうか．G が(＊)を満たすというだけでは，恐らく何の有効な解答も期待し得ないであろう($PSL(n,q)$ $(q=p^e)$ の放物的部分群を思い浮べよ)．しかし，Glauberman は条件(＊)のもとで

(＊＊) G が p 可解群 $(p\geqq 5)\Longrightarrow G\triangleright Z(J(P))$

($Z(J(P))$ は§7.3, d) で定義した $J(P)$ の中心)

という驚くべき定理を証明した(1966年)．この結果は，"奇数位数の群の可解性"の原証明の重要な一部(全証明約250ページのうちの約50ページ)の20-30ページを一挙に短縮する程の強力なものであった．その後，(＊＊)は，G の p 可解性の条件がもう少しゆるめられて一般化され，近年の有限単純群論で大切な役割を果たしている．この§7.4, b) とつぎの§7.4, c) の目的は，一般化された形でこの Glauberman の定理を証明することである．

有限群 G の p 群 V への作用に関する簡単な事柄から始めよう．

補題 7.32 有限群 G が標数 p の体の上の線型空間 V の上に作用しているとする．このときつぎの(i), (ii)が成り立つ:

(i) G が p 群ならば，$C_V(G)\neq 0$,

(ii) (G, V) が既約ならば，$O_p(G)\subseteqq C_G(V)$.

証明 (i) $V \ni v \neq 0$ とする．$V_0 = \{\sum_{x \in G} \alpha_x v^x \mid \alpha_x \in F_p\}$ (F_p は素体) とおくと，V_0 は基本 Abel p 群である．G は $V_0 - \{0\}$ に作用し，その元の数は p と素だから，補題 2.4 により G は $V_0 - \{0\}$ の上に固定点をもつ．とくに $C_V(G) \neq 0$ である．

(ii) (i) により $C_V(O_p(G)) \neq 0$ である．また $C_V(O_p(G))$ は G 不変である．よって (G, V) の既約性により，$C_V(O_p(G)) = V$ すなわち $O_p(G) \subseteq C_G(V)$ を得る．∎

$G \triangleright N$ のとき，$O_p(G \bmod N)$ によって G から G/N への自然準同型による $O_p(G/N)$ の逆像を表わすことにしよう：

$$G \triangleright N, \quad O_p(G/N) = K/N \quad \text{のとき} \quad K = O_p(G \bmod N).$$

補題 7.33 有限群 G が p 群 V に作用しているとする．

$$V = V_0 \supsetneqq V_1 \supsetneqq \cdots \supsetneqq V_{n-1} \supsetneqq V_n = 1$$

を V の G 主組成列とするとき，

$$\bigcap_{i=0}^{n-1} C_G(V_i/V_{i+1}) = O_p(G \bmod C_G(V))$$

である．

証明 $N = O_p(G \bmod C_G(V))$，$\bar{V}_i = V_i/V_{i+1}$，$N_i = C_G(\bar{V}_i)$ ($i = 0, 1, 2, \cdots, n-1$) とおく．$NN_i \triangleleft G$ であるから $NN_i/N_i \triangleleft G/N_i$．また $C_G(V) \subseteq N \cap N_i$ より，$NN_i/N_i \simeq N/N \cap N_i$ は p 群である．よって $NN_i \subseteq O_p(G \bmod N_i)$．一方，補題 7.32 により $O_p(G \bmod N_i) \subseteq C_G(\bar{V}_i)$．したがって

$$N \subseteq \bigcap_{i=0}^{n-1} C_G(\bar{V}_i)$$

を得る．逆の包含関係を示すためには，$D = \bigcap_{i=0}^{n-1} C_G(\bar{V}_i)$ とおく．$D \triangleleft G$ は明らかである．D の位数が p と素な元は，補題 7.12 により，$C_G(V)$ に含まれるから，$D/C_G(V)$ は p 群である．よって $D \subseteq O_p(G \bmod C_G(V))$ を得る．∎

G の p 群 V への作用がつぎの条件を満たすとき，この作用は p **安定的**であるという：

$$[V, x, x] = 1 \quad (x \in G) \Longrightarrow x \in O_p(G \bmod C_G(V)).$$

上の補題 7.33 により，$x \in O_p(G \bmod C_G(V))$ は，V の各 G 主組成因子への x の作用が自明なものであることを示している．交換子条件 $[V, x, x] = 1$ の意

味を説明しよう．V を基本 Abel p 群(＝標数 p の素体の上の有限次元線型空間)とする．$G\ni x$ に対して，V から V への写像

$$V\ni v\longmapsto [v,\underbrace{x,x,\cdots,x}_{r}]\in V$$

は，V の $(x-1)^r$ なる自己準同型(線型変換)を表わす．実際，

$$[v,x]=v^{-1}v^x=v^{x-1},$$
$$[v,x,x]=[[v,x],x]=(v^{x-1})^{x-1}=v^{(x-1)^2},$$
$$\vdots$$
$$[v,\underbrace{x,\cdots,x}_{r}]=[[v,\underbrace{x,\cdots,x}_{r-1}],x]=(v^{(x-1)^{r-1}})^{x-1}=v^{(x-1)^r}$$

である．したがって，V が基本 Abel 群のとき，$[V,x,x]=1$ なる条件は，x が V 上へひき起す線型変換の最小多項式が $(X-1)^2$ または $X-1$ (このときは，もちろん $x\in C_G(V)$) であることを示す．

まず，p 安定的でない作用の例をあげよう．

例 7.5　V を標数 p の有限体上の 2 次元線型空間，$SL(V)$ を V の特殊線型群とする．$SL(V)$ の V への自然な作用は p 安定的ではない．実際，$G=SL(V)$ の V への作用は既約であり，$O_p(G \bmod C_G(V))=1$ である．一方，G の位数 p の元 x は，V の基底を適当にとれば，

$$\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}$$

の形の行列で表わされるから，x の最小多項式は $(X-1)^2$ である．これは，上の注意により $[V,x,x]=1$ を示す．$x\notin O_p(G \bmod C_G(V))=1$ であるから，G の V への作用は p 安定的ではない．——

この例のように，p 安定的でない作用と標数 p の有限体上の線型群(特殊線型群，斜交群，直交群など)の自然な表現とは密接な関係がある．しかし，ここでは p 安定的作用の例をあげるために，つぎの補題を述べるにとどめる．

補題 7.34　p を奇素数とする．G の或る p 群への作用が p 安定的でないならば，G はつぎの性質を満たす部分群 H,K を含む：

(7.66)　　$$H\rhd K,\qquad H/K\simeq SL(2,p).$$

例題 7.10　有限群 G がつぎの (i), (ii), (iii) の一つを満たすとき，G の任意の p 群(p は奇素数)への作用は，p 安定的である：

(i) G の位数は奇数,

(ii) G は p 可解群 ($p \geqq 5$),

(iii) G の Sylow 2 部分群が，Abel 群または正 2 面体群.

[証明]　(i) $SL(2,p)$ の位数は偶数だから，奇数位数の群 G は，(7.66) を満たす部分群 H, K を含み得ない. (ii) $p \geqq 5$ のとき，$SL(2,p)$ は p 可解群ではない. p 可解群の部分群や剰余群は p 可解群だから，G が p 可解群ならば，G は (7.66) を満たす H, K を含み得ない. (iii) $SL(2,p)$ の Sylow 2 部分群は 4 元数型の群である. 一方，Abel 群や正 2 面体群の部分群や剰余群は，やはり Abel 群または正 2 面体群である. さらに Abel 群や正 2 面体群は 4 元数型の群と同型な部分群を含まない. これらから (iii) を満たす G は，(7.66) を満たす H, K を含み得ない. ▌

さて，補題 7.34 は，$SL(2,q)$ の生成系に関するつぎの Dickson の定理を用いて証明される.

Dickson の定理　$q=p^e$ (p は奇素数)，λ を素体 F_p 上の F_q の生成元，L を

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$$

によって生成される $SL(2,q)$ の部分群とする. このときつぎの (i) または (ii) が成り立つ:

(i) $L = SL(2,q)$,

(ii) $q = 9, \quad L \simeq SL(2,5)$.

(i), (ii) いずれの場合も，L は $SL(2,p)$ と同型な部分群を含む. ——

この Dickson の定理の証明は少し複雑で長くなるので省略するが，証明を知りたい方は，D. Gorenstein: Finite Groups, Harper & Row, New York, pp. 44-55 を参照されたい. ここでは，Dickson の定理から上の補題 7.34 が如何に導かれるかを説明しておこう. まず Dickson の定理はつぎのようにいいかえることができる.

定理 7.23　p を奇素数とする. G が基本 Abel p 群 V の上に忠実かつ既約に作用しているとする. G が

(α) $G = \langle x_1, x_2 \rangle$,

(β) $[V, x_i, x_i] = 1 \quad (i=1,2)$

なる条件を満たせば，つぎの (i) または (ii) が成り立つ:

(i) $G \simeq SL(2,q) \quad (q=p^e)$,

(ii) $p=3$ で $G \simeq SL(2,5)$.

とくに (i), (ii) いずれの場合でも G は $SL(2,p)$ と同型な部分群を含む.

証明 V を標数 p の素体の上の線型空間とみなし，x_1, x_2 は V の線型変換と考えることにする．$V_i=C_G(x_i)$，$W_i=V_i(x_i-1)$ $(i=1,2)$ とおく．(ii) により，$(x_i-1)^2=0$ だから，$W_i \subseteqq V_i$ を得る．$V_i=\mathrm{Ker}(x_i-1)$ であるから，$\dim V = \dim W_i + \dim V_i$，したがって

$$\dim V \leqq 2 \dim V_i \qquad (i=1,2) \tag{7.67}$$

である．一方 (α) により $V_1 \cap V_2$ は G 不変だから，(G, V) の既約性から $V_1 \cap V_2 = 0$，よって

$$\dim V_1 + \dim V_2 \leqq \dim V \tag{7.68}$$

を得る．(7.67), (7.68) より

$$\dim V_1 = \dim V_2 = \frac{1}{2}\dim V$$

である．$\dim V_1 = \dim V_2 = m$ とおく．$V=V_1 \oplus V_2$ (直和) であるから，

$$V_1 = W_1 = (x_1-1)V_2, \quad V_2 = W_2 = (x_2-1)V_1$$

である．V_2 の基底 $v_1, v_2, \cdots, v_m$ をとり，

$$v_{m+i} = v_i(x_1-1)$$

とおくと，$v_1, v_2, \cdots, v_m, v_{m+1}, \cdots, v_{2m}$ は V の基底で，線型変換 x_1, x_2 はこの基底に関してつぎの行列で表わされる:

$$\begin{bmatrix} E_m & E_m \\ 0 & E_m \end{bmatrix}, \quad \begin{bmatrix} E_m & 0 \\ R & E_m \end{bmatrix}.$$

(G, V) の既約性から，R は F_p 上既約な行列であることが容易にわかる．このとき，Schur の補題により $F_p[R]$ は体である．$K=F_p[R]$ とおく．V を基底 v_1 $v_2, \cdots, v_{2m}$ に関して F_p 上の $2m$ 次元数ベクトル空間 ${F_p}^{2m}$ と同一視すると，

$$x \longmapsto x\begin{bmatrix} S & 0 \\ 0 & S \end{bmatrix} \qquad (S \in K, \ \ x \in {F_p}^{2m})$$

として，V は K 上の 2 次元線型空間とみなすことができる．このとき，G は V の K 上の線型変換をひき起し，x_1, x_2 に対応する行列は，

$$\begin{bmatrix}1&1\\0&1\end{bmatrix},\quad \begin{bmatrix}1&0\\\lambda&1\end{bmatrix}\qquad (K=F_p(\lambda))$$

である．よってこの定理は，Dickson の定理からでる．▌

つぎに一般的補題を一つ証明しよう．

補題 7.35 (Baer)　G を有限群，p を素数とする．K は G の共役類で

$$K\ni x,y \Longrightarrow \langle x,y\rangle = p\ 群$$

なる条件を満たすとする．このとき，$K\subseteqq O_p(G)$．

証明 (Alperin-Lyons)　$K\subsetneqq O_p(G)$ と仮定して矛盾を導こう．$K\subsetneqq O_p(G)$ より

(7.69)
$$K\cap P \neq K\cap Q$$

なる $P,Q\in \mathrm{Syl}_p(G)$ が存在することがわかる．実際，そうでなければ，G の任意の元 x に対して

$$K\cap P = K\cap P^x$$

であるから，

$$K\cap P \subseteqq \bigcap_{x\in G} P^x = O_p(G).$$

K は共役類だから，これは $K\subseteqq O_p(G)$ を示し，仮定に反する．さて，(7.69) を満たす $P,Q\in \mathrm{Syl}_p(G)$ で

$$|K\cap P\cap Q|$$

が最大になるように P,Q をとろう．

$$D = \langle K\cap P\cap Q\rangle^{1)}$$

とおくと，明らかに

(7.70)
$$D\subseteqq P\cap Q,\qquad K\cap D = K\cap P\cap Q,\qquad D=\langle K\cap D\rangle$$

である．つぎに

(7.71)
$$K\cap P - D\ni \exists x,\qquad x\in N_G(D),$$

(7.72)
$$K\cap Q - D\ni \exists y,\qquad y\in N_G(D)$$

を示そう．

$$D = P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_{n-1} \subsetneqq P_n = P,\qquad [P_i:P_{i-1}] = p$$

とすると，$K\cap P_0\subseteqq D$，$K\cap P_n\subsetneqq D$ であるから，

$$K\cap P_{i-1}\subseteqq D,\qquad K\cap P_i \subsetneqq D$$

---

1)　$K\cap P\cap Q$ が空集合のとき，$D=1$ と約束する．

なる i が存在する．$K\cap P_i-D\ni x$ とすると $P_i\rhd P_{i-1}$ だから，$x\in N_G(P_{i-1})$．ところで $K\cap P_{i-1}=K\cap D$ であるから，

$$(K\cap D)^x=(K\cap P_{i-1})^x=K\cap P_{i-1}{}^x=K\cap P_{i-1}=K\cap D.$$

よって (7.70) により $x\in N_G(D)$ である．すなわち (7.71) が成り立つ．同様に (7.72) が示される．定理の仮定により $\langle x,y\rangle$ は p 群だから，

$$R_0=\langle x,y\rangle D$$

とおくと，(7.71), (7.72) により R_0 も p 群である．$R_0\subseteqq R\in \mathrm{Syl}_p(G)$ とすると，(7.71) により

$$K\cap P\cap R\supseteqq \{x, K\cap P\cap Q\}\supsetneqq K\cap P\cap Q$$

であるから，P, Q のとり方から，$K\cap P=K\cap R$．同様に

$$K\cap Q\cap R\supseteqq \{y, K\cap P\cap Q\}\supsetneqq K\cap P\cap Q$$

より，$K\cap Q=K\cap R$．したがって $K\cap P=K\cap Q$ となり矛盾である．▌

補題 7.34 の証明 G を最小位数の反例とする．さらに V を G が p 安定的に作用しない最小位数の p 群とする．このとき，

$$[V,x,x]=1,\qquad x\notin O_p(G \bmod C_G(V))$$

なる $x\in G$ が存在する．

(α) G の V への作用は忠実かつ既約である．

[証明] (G, V) は既約でないとしよう．

$$V=V_0\supsetneqq V_1\supsetneqq\cdots\supsetneqq V_{n-1}\supsetneqq V_n=1$$

を V の G 主組成列とする．$\bar{V}_i=V_i/V_{i+1}$，$N_i=C_G(\bar{V}_i)$ とおくと，補題 7.32 の (ii) により $O_p(G \bmod N_i)=N_i$ である．また $|\bar{V}_i|<|V|$ より，G の $\bar{V}_i$ への作用は p 安定的である．よって $[\bar{V}_i,x,x]=1$ より $x\in O_p(G \bmod N_i)=N_i$．このとき補題 7.33 により $x\in O_p(G \bmod C_G(V))$ となり矛盾である．したがって，(G, V) は既約である．$C=C_G(V)\neq 1$ とすると，$\bar{G}=G/C$ の V への作用は p 安定的でないから，$|\bar{G}|<|G|$ より，$\bar{G}$ は

$$\bar{H}\rhd\bar{K},\qquad \bar{H}/\bar{K}\simeq SL(2,p)$$

なる部分群 $\bar{H},\bar{K}$ を含む．$\bar{H}=H/C$，$\bar{K}=K/C$ とすると

$$H\rhd K,\qquad H/K\simeq SL(2,p)$$

となり，G が反例であることに反する．▌

(β) x の或る共役 y が存在して，$G=\langle x,y\rangle$.

[証明] (G, V) は忠実かつ既約だから，補題7.32により $O_p(G)=1$. また補題7.35により x の或る共役 y が存在して，$G_1=\langle x, y\rangle$ は p 群ではない．このとき，G_1 の V への作用は p 安定的でない．なぜならば，(G_1, V) が p 安定的ならば，$[V, x, x]=1$ より，$x\in O_p(G_1 \bmod C_{G_1}(V))=O_p(G_1)$ となり，$G_1=\langle x, y\rangle =\langle y\rangle O_p(G_1)$ が p 群となり，矛盾である．$G\neq G_1$ ならば，G_1 したがって G が

$$H \triangleright K, \qquad H/K \simeq SL(2, p)$$

なる部分群 H, K を含むことになり矛盾である．▌

(γ) (α), (β) により (G, V) は定理7.23のすべての仮定を満たす．よって G は $SL(2, p)$ と同型な部分群を含むことになり矛盾である．▌

c) Glauberman の ZJ 定理

P を p 群とする．§7.3, d) で定義されたものと少し異なる Thompson 部分群 $J(P)$ を定義しよう．P の可換部分群の最大位数を $d(P)$ と書く．P の位数 $d(P)$ の可換部分群全体の集合を $\mathcal{A}(P)$ とする．このとき，$J(P)$ を

$$J(P) = \langle A \mid A\in \mathcal{A}(P)\rangle$$

によって定義する．

つぎの (7.73), (7.74), (7.75) は定義から容易にわかる：

(7.73) $\qquad A\in\mathcal{A}(P) \Longrightarrow C_P(A)=A$ とくに $A \supseteqq Z(P)$,

(7.74) $\qquad J(P)$ は P の特性部分群である，

(7.75) $\qquad J(P)\subseteqq Q \subseteqq P \Longrightarrow J(P)=J(Q)$.

$J(P)$ の取り扱いにおいてつぎの二つの定理は基本的である．

定理 7.24 (Thompson) $A\in\mathcal{A}(P)$，$P\ni x$，$M=[x, A]$ とおく．M が可換部分群ならば，$MC_A(M)\in\mathcal{A}(P)$.

証明 $MC_A(M)$ は明らかに可換部分群だから

$$|MC_A(M)| \geqq |A|$$

を示せば十分である．ところで $M\cap C_A(M)=C_M(A)$ であるから，

$$|MC_A(M)| = |M||C_A(M)|/|M\cap C_A(M)| = |M||C_A(M)|/|C_M(A)|.$$

よって

$$|M/C_M(A)| \geqq |A/C_A(M)|$$

を示せばよい．それには，$A\ni u, v$ のとき，

$$[x, u]^{-1}[x, v]\in C_M(A) \Longrightarrow u^{-1}v\in C_A(M)$$

を示せば十分である．まず

$$[x,u]^{-1}[x,v]=[x,u^{-1}v]$$

を示そう．実際，$y=[x,u]^{-1}[x,v]$ とおくと，

$$y=(x^{-1}x^u)^{-1}(x^{-1}x^v)=x^{-u}x^v.$$

$y\in C_M(A)$ より $y=y^{u^{-1}}=(x^{-u}x^v)^{u^{-1}}=x^{-1}x^{u^{-1}v}=[x,u^{-1}v]$ である．$[x,u]^{-1}[x,v]\in C_M(A)$ より

$$[x,u^{-1}v,A]=1.$$

明らかに $[u^{-1}v,A,x]=1$．よって3部分群補題5.8により，$[A,x,u^{-1}v]=1$．すなわち $u^{-1}v\in C_A(M)$ である．▌

$J(P)$ の中心 $Z(J(P))$ を $ZJ(P)$ によって表わすことにする．

定理 7.25 (Glauberman-Thompson) P を p 群，p は奇素数とする．B を $P\triangleright B$，$B'\subseteq ZJ(P)\cap Z(B)$ (B' は B の交換子群) なる P の部分群とする．$A\in\mathscr{A}(P)$，$[B,A,A]\neq1$ のとき，つぎの性質を満たす $A^*\in\mathscr{A}(P)$ が存在する：

(i) $A\cap B\subsetneqq A^*\cap B$,

(ii) $[A^*,A,A]=1$.

証明 $P=AB$ と仮定してよい．このとき，

$$B'\subseteq Z(P) \tag{7.76}$$

である．

整数 $i\geqq0$ に対して

$$[B,A\,;0]=B,\qquad [B,A\,;i]=[B,\underbrace{A,A,\cdots,A}_{i}]\quad(i>0)$$

によって $[B,A\,;i]$ を定義する．r を

$$[B,A\,;r]=1$$

なる最小の正整数とする．$P=AB$ は巾零群だから，このような r が存在し，また仮定 $[B,A,A]\neq1$ により

$$r\geqq3$$

である．$[B,A\,;r-1]\neq1$ であるから，$[B,A\,;r-3]\ni x$ を $[x,A,A]\neq1$ なるようにとることができる．$M=[x,A]$ とおく．このとき，

$$M\subseteq B,\qquad [M,A\cap B]=1,\qquad M\nsubseteq A \tag{7.77}$$

である．なぜなら，$B\triangleleft P$ より，$[B,A\,;i]\subseteq B$ ($i\geqq0$)，とくに $M\subseteq B$ となる．

また $B'\subseteqq Z(P)$ より $[A\cap B, x, A]\subseteqq[B, B, A]=[B', A]=1$, $[A, A\cap B, x]=1$. よって 3 部分群補題 5.8 により $[M, A\cap B]=[x, A, A\cap B]=1$ を得る. また $[x, A, A]\neq 1$ より $M\subsetneqq A$ である. さて

(7.78) $M=[x, A]$ が可換群ならば $A^*=MC_A(M)$ が求めるものであることを示そう. 実際, そのとき定理 7.24 により $A^*\in\mathscr{A}(P)$, さらに, (7.77) により

$$A^*\cap B = MC_A(M)\cap B \supseteqq M(C_A(M)\cap B) \supseteqq M(A\cap B) \supsetneqq A\cap B,$$

$$[A^*, A, A] = [MC_A(M), A, A] = [M, A, A] \subseteqq [B, A\,; r] = 1$$

である. とくに, $[B, A\,; r-2]$ が可換群ならば, $M=[x, A]\subseteqq[B, A\,; r-2]$ だから, 定理が成り立つ. よって,

(7.79) $[B, A\,; r-2]$ は 非可換群

と仮定してよい. $\bar{P}=P/B'$ とおく. $K_0(\bar{P})=\bar{P}$, $K_1(\bar{P})$, $\cdots$ を $\bar{P}$ の降中心列とするとき,

$$K_i(\bar{P}) = [\bar{B}, \bar{A}\,; i] \qquad (i=1, 2, \cdots)$$

が容易にわかる ($\bar{B}, \bar{A}$ が Abel 群, $\bar{B}\triangleleft\bar{P}$ に注意して (5.4) を繰返し用いよ!). $K_r(\bar{P})=[\bar{B}, \bar{A}\,; r]=1$, $B'\subseteqq Z(P)$ より $K_{r+1}(P)=1$ である. このとき, m を $(r+1)/2$ 以下の最大の整数とすると,

$$K_m(P) \quad \text{は} \quad \text{可換群} \qquad (\text{問 } 5.14 \text{ 参照})$$

であるから, (7.79) により

$$\frac{r+1}{2} \geqq r-1, \qquad \therefore \quad r = 3$$

を得る. よって

(7.80) $$[B, A\,; 3] = 1$$

である. $A\ni u, v$ に対して

$$[[x, u], [x, v]] = 1$$

を示そう. Witt の恒等式 (5.16) により

$$[[x, u], [x, v]]^{u^{-1}}\cdot[u^{-1}, [x, v]^{-1}, x]^{[x, v]}\cdot[[x, v]^{-1}, x^{-1}, u^{-1}]^{x} = 1$$

であるが, $B'\subseteqq Z(P)$ に注意すれば,

$$[[x, u], [x, v]]\cdot[u^{-1}, [x, v]^{-1}, x] = 1.$$

したがって

(7.81)
$$[[x,u],[x,v]] = [u^{-1},[x,v]^{-1},x]^{-1}$$
$$= [[u^{-1},[x,v]^{-1}]^{-1},x]$$
$$(B \text{ の巾零クラス } \leqq 2,\ \text{問 5.7 参照})$$
$$= [[[x,v]^{-1},u^{-1}],x]$$

である．ところで(7.80)により $[\bar{B},\bar{A}]\bar{A}$ は巾零クラスが高々2であるから，

$$[[\bar{x},\bar{v}]^{-1},\bar{u}^{-1}] = [\bar{x},\bar{v},\bar{u}].$$

また，$\bar{A}$, $[\bar{x},\bar{A}]$ は可換群だから，

$$[\bar{x},\bar{v},\bar{u}] = [\bar{x},\bar{u},\bar{v}].$$

よって

$$[[x,v]^{-1},u^{-1}] = [x,v,u]z = [x,u,v]z' \qquad (z,z' \in B').$$

(7.81)と $B' \subseteqq Z(P)$ より

$$[[x,u],[x,v]] = [x,v,u,x] = [x,u,v,x]. \tag{7.82}$$

u, v に関する対称性によって

$$[[x,v],[x,u]] = [x,u,v,x]. \tag{7.83}$$

(7.82), (7.83)より

$$[[x,u],[x,v]] = [[x,v],[x,u]] = [[x,u],[x,v]]^{-1}.$$

よって

$$[[x,u],[x,v]]^2 = 1.$$

p は奇素数だから，$[[x,u],[x,v]]=1$，すなわち $[x,A]$ は可換群である．▌

系　P, B を定理7.25の通りとするとき，$[B,A,A]=1$ なる $A \in \mathscr{A}(P)$ が存在する．

証明　$|A \cap B|$ が最大になるように $A \in \mathscr{A}(P)$ を選べばよい．▌

G を $O_p(G) \neq 1$ なる群としよう．G の任意の正規 p 部分群 P に対して，G の P への(共役による)作用が p 安定的のとき，G を p **安定群**ということにしよう．すなわち，

$$G \triangleright P = p \text{ 部分群},\quad G \ni x,\quad [P,x,x]=1 \Longrightarrow x \in O_p(G \bmod C_G(P))$$

なる条件を満たすとき，G は p 安定群である．例題7.10により，奇数位数の群 p 可解群($p \geqq 5$, $p=3$ でも Sylow 2 部分群が Abel 群や正2面体群ならよい)は p 安定群である．

補題 7.36 (Glauberman)　p を奇素数，G を p 安定群，$P \in \mathrm{Syl}_p(G)$ とする．

G の任意の正規 p 部分群 B に対して，$G \triangleright B \cap ZJ(P)$ である：

$$G \triangleright B \subseteqq O_p(G) \Longrightarrow G \triangleright B \cap ZJ(P).$$

証明 補題が成立しないと仮定して矛盾を導こう．B を

$$G \triangleright B \subseteqq O_p(G), \quad G \not\triangleright B \cap ZJ(P)$$

なる最小位数の部分群とする．まず

(7.84) $$B' \subseteqq ZJ(P) \cap Z(B)$$

であることを示そう．$Z = ZJ(P)$ とおく．$B_1 = \langle (Z \cap B)^x \mid x \in G \rangle$ とすると，

$$G \triangleright B_1 \subseteqq B, \quad Z \cap B_1 = Z \cap B$$

であるから，B の最小性により $B = B_1$ でなければならない：

(7.85) $$B = \langle (Z \cap B)^x \mid x \in G \rangle.$$

また，B の最小性により $G \triangleright Z \cap B'$ である．$[B, Z \cap B] \subseteqq Z \cap B'$ であるから，$Z \cap B \subseteqq C_G(B/Z \cap B') \triangleleft G$．(7.85) により $B \subseteqq C_G(B/Z \cap B')$．とくに $B' \subseteqq Z$，$[B', Z \cap B] = 1$ を得る．再び (7.85) により $[B', B] = 1$ すなわち $B' \subseteqq Z(B)$ である．よって (7.84) が示された．

$L = \bigcap_{x \in G} N_G(Z \cap B)^x$ とおく．このとき，

$$B \subseteqq L \triangleleft G,$$
$$Z \cap B \triangleleft K \triangleleft G \Longrightarrow K \subseteqq L$$

は，L の定義から容易にわかる．また

(7.86) $$O_p(G/L) = 1$$

である．実際，$O_p(G/L) = K/L$ とおくと，$G \triangleright K = (P \cap K)L$．明らかに $(P \cap K)L \triangleright Z \cap B$ だから，(7.85) により $K \subseteqq L$，すなわち $O_p(G/L) = 1$ である．つぎに

(7.87) $$[B, A, A] = 1, \quad A \in \mathscr{A}(P) \Longrightarrow A \subseteqq L$$

を示そう．G は p 安定群だから，$A \subseteqq O_p(G \bmod C_G(B))$ である．一方，$Z \cap B \triangleleft C_G(B) \triangleleft G$ だから (7.85) により $C_G(B) \subseteqq L$．したがって $A \subseteqq O_p(G \bmod C_G(B)) \subseteqq O_p(G \bmod L) = L$ である．つぎに

$$J(P \cap L) \neq J(P), \quad ZJ(P \cap L) \supseteqq Z$$

を示そう．$J(P) = J(P \cap L)$ ならば $G = N_G(J(P \cap L))L = N_G(J(P))L$．$N_G(J(P)) \triangleright Z \cap B$ だから，$G \triangleright Z \cap B$ となり矛盾である．よって $J(P \cap L) \neq J(P)$．ところで，(7.84) と定理 7.25 の系により $[B, A, A] = 1$ なる $A \in \mathscr{A}(P)$ が存在する．このとき，(7.87) により $A \subseteqq L$，よって $Z \subseteqq A \subseteqq J(P \cap L)$，すなわち $Z \subseteqq ZJ(P \cap L)$

である．さて $X=ZJ(P\cap L)$ とおくと，$G=N_G(X)L$ であるから，(7.85) により $X\supseteqq B$ である．また $J(P\cap L)\neq J(P)$ であるから，$A_1\subsetneqq L$ なる $A_1\in\mathcal{A}(P)$ が存在する．このような A_1 で $|A_1\cap B|$ が最大になるようなものをとる．このとき，(7.87) により $[B, A_1, A_1]\neq 1$ である．よって定理 7.25 により $A_1\cap B\subsetneqq A^*\cap B$，$[A^*, A, A]=1$ なる $A^*\in\mathcal{A}(P)$ が存在する．このとき，A_1 のとり方から $A^*\subseteqq L$，とくに $X\subseteqq A^*$ である．ところで $X\supseteqq B$ だったから，

$$[B, A_1, A_1]\subseteqq[X, A_1, A_1]\subseteqq[A^*, A_1, A_1]=1$$

を得るが，$[B, A_1, A_1]\neq 1$ であるから，これは矛盾である．▌

定理 7.26(Glauberman の ZJ 定理)　G を $F^*(G)$ が p 群であるような p 安定群(p は奇素数)とする．このとき $G\triangleright ZJ(P)$ $(P\in \mathrm{Syl}_p(G))$ である．

証明　$B=F^*(G)$ とおく．補題 7.36 により $G\triangleright B\cap Z$，$Z=ZJ(P)$ である．Z，$B\lhd P$ より $[Z, B]\subseteqq Z\cap B$ であるから，

$$Z\subseteqq C_G(B/Z\cap B)\cap C_G(Z\cap B).$$

ところで，$C_G(B/Z\cap B)\cap C_G(Z\cap B)$ の位数が p と素な元は，補題 7.12 により，$C_G(B)$ に属する．一方，(7.52) により $C_G(B)\subseteqq B$ であるから，$C_G(B/Z\cap B)\cap C_G(Z\cap B)$ は p 群である．よって

$$C_G(B/Z\cap B)\cap C_G(Z\cap B)\subseteqq B.$$

すなわち $Z\subseteqq B$．よって $G\triangleright Z\cap B=Z$ である．▌

この Glauberman の ZJ 定理から，定理 7.15 をもう少し簡単な形にしたつぎの定理が導かれる．

Glauberman の定理　G を有限群，p を奇素数，$P\in \mathrm{Syl}_p(G)$ とする．このとき，$N_G(ZJ(P))$ が p 巾零ならば，G も p 巾零である．——

この定理の証明は，定理 7.15 の証明の前半の真似をすれば，その証明の (γ) の段階で，ZJ 定理が適用できて矛盾が生じることから得られる．定理 7.15 の証明の復習を兼ねて読者自ら試みられたい．

d）素数 2 に対する信号関手定理

この項では，ZJ 定理その他本章で説明してきた結果の応用として，素数 2 に対する信号関手定理(これを，以後簡単に 2 信号関手定理と略称する)の H. Bender による証明を紹介しよう．この証明の中に現われる Bender の卓抜なアイデアは，可換な Sylow 2 部分群をもつ有限単純群の分類定理やその他の有限

群論の重要な結果に極めて有効に応用されているものである.

G を有限群, $\mathscr{M}$ を G の部分群からなる集合でつぎの性質をもつものとする:

$$\begin{aligned}&\mathscr{M} \ni A, \quad X = A \text{ の特性部分群} \neq 1 \\ &\Longrightarrow N_B(X) \subseteq A \qquad (\forall B \in \mathscr{M}).\end{aligned} \tag{7.88}$$

例 7.6 G を有限単純群, $\mathscr{M}$ を G の極大部分群全体の集合とすると, $\mathscr{M}$ は (7.88) を満たす.

定理 7.27 (Bender) G を有限群, $\mathscr{M}$ を (7.88) を満たす G の部分群の集合とする. $A, B \in \mathscr{M}$, S, T をそれぞれ $F^*(A), F^*(B)$ の部分群で

$$S \supseteq E(A), \qquad C_{F^*(A)}(S) \subseteq S,$$
$$T \supseteq E(B), \qquad C_{F^*(B)}(T) \subseteq T$$

なる性質をもつものとする. このとき, $S \subseteq B$, $T \subseteq A$ ならば, つぎの (i), (ii) のいずれかが成り立つ:

(i) $A = B$,

(ii) $F^*(A), F^*(B)$ は同じ素数 p に対する p 群である. ——

この定理の証明において, $F^*(G)$ の基本性質

$$C_G(F^*(G)) \subseteq F^*(G) \qquad (\text{定理 } 5.5) \tag{7.89}$$

と, 補題 7.12 が繰返し用いられるであろう. また, つぎの記号も用いる. 有限群 G の位数を割る素数全体の集合を $\pi(G)$ によって表わす:

$$\pi(G) = \{p = \text{素数} \mid p \mid |G|\}.$$

さらに巾零群 X に対して $O_p(X), O_{p'}(X)$ をそれぞれ簡単に $X_p, X_{p'}$ で表わすことがある:

$$X_p = O_p(X), \qquad X_{p'} = O_{p'}(X).$$

このとき, X は巾零群だから

$$X = X_p \otimes X_{p'}$$

である.

定理 7.27 の証明 まず仮定により

$$F^*(A) = F(A)E(A) \supseteq S = F(S)E(A), \qquad C_{F(A)}(F(S)) \subseteq F(S),$$
$$F^*(B) = F(B)E(B) \supseteq T = F(T)E(B), \qquad C_{F(B)}(F(T)) \subseteq F(T)$$

である. 以下 $A \neq B$ と仮定して (ii) が成り立つことを示そう.

(α) $E(A) = E(B) = 1$.

[証明] $E(B)\subseteqq A$ だから，補題5.15により

$$E(A) = [E(A), E(B)]C_{E(A)}(E(B)). \tag{7.90}$$

また，$E(A)\subseteqq B$ および $E(A)\cap F(B)$ は $E(A)$ 不変であることに注意すれば，

$$[E(A), F(T)] \subseteqq E(A)\cap F(B) \subseteqq Z(E(A)).$$

3部分群補題5.8(あるいは(5.21))により，これは

$$[E(A), F(T)] = 1$$

を示す．$\pi(F(T))\ni p$ とすると，

$$[E(A), F(T)_p] = 1, \quad C_{F(B)_p}(F(T)_p) \subseteqq F(T)_p$$

である．x を $E(A)$ の位数が p と素な元とすると，$[x, F(T)_p]=1$ であるから，x の $F(B)_p$ への作用に対して補題7.12の(iv)を適用すれば，$[x, F(B)_p]=1$ を得る．$E(A)$ はそのような元によって生成されるから，$[E(A), F(B)_p]=1$ である．よって

$$[E(A), F(B)] = 1$$

を得る．したがって(7.89)を用いて

$$C_{E(A)}(E(B)) \subseteqq C_B(F^*(B)) \subseteqq F(B).$$

よって(7.90)から，$E(A)\subseteqq E(B)F(B)$ を得るが，両辺の交換子をとれば $E(A)\subseteqq E(B)$ となる．A と B の対称性により，$E(B)\subseteqq E(A)$ も成り立つから，$E(A)=E(B)$ を得る．もし $E(A)=E(B)\neq 1$ ならば，(7.88)により $B=N_B(E(B))=N_B(E(A))\subseteqq A$．再び A と B の対称性によって $A=B$ となる．これは矛盾である．▌

(β) $\pi(F(A)) = \pi(F(B))$.

[証明] $p\in\pi(F(A))-\pi(F(B))$ とすると，$[F(S)_p, F(T)]\subseteqq F(A)\cap F(B)=1$. $F(S)_p$ の $F(B)$ への作用に対して，補題7.12の(iv)を適用すれば，$[F(S)_p, F(B)]=1$ を得る．よって(7.89)により

$$F(S)_p \subseteqq C_B(F(B)) \subseteqq F(B) \qquad (E(B)=1 \text{ に注意})$$

となり，これは $p\in\pi(F(A))-\pi(F(B))$ に矛盾する．▌

$|\pi(F(A))|=|\pi(F(B))|=1$ を示せば，(β)により(ii)が成り立つことになるから，以下 $|\pi(F(A))|=|\pi(F(B))|\geqq 2$ と仮定して矛盾を導こう．

(γ) $F(A)\subseteqq B$, $F(B)\subseteqq A$.

[証明] $\pi(F(A))\ni p$ とする．$[F(S)_p, F(T)_{p'}]\subseteqq F(A)_p\cap F(B)_{p'}=1$ である

から，$F(T)_{p'}$ の $F(A)_p$ への作用に補題 7.12 の (iv) を適用して，$[F(A)_p, F(T)_{p'}]=1$ を得る．$|\pi(F(B))|\geqq 2$ であるから，$F(T)_{p'}\supseteqq Z(F(B)_{p'})\neq 1$．よって，(7.88) により

$$F(A)_p \subseteq C_A(Z(F(B))_{p'}) \subseteq N_A(Z(F(B))_{p'}) \subseteq B$$

($Z(F(B))_{p'}$ は B の特性部分群であることに注意)．

これから，$F(A)\subseteq B$ を得る．同様にして $F(B)\subseteq A$ である．▌

(δ) $\pi(F(A))=\pi(F(B))\ni p$, $P=F(A)_p$, $Q=F(B)_p$ とおく．K を，$C_B(Q)$ の位数が p と素な元全体によって生成される部分群とするとき，$[P,K]=1$ である．

[証明] $P\subseteq B$, $[P, F(B)_{p'}]\subseteq P\cap F(B)_{p'}=1$ であるから，$PF(B)$ は巾零群である．明らかに

$$[F(B)_{p'}, P, C_B(Q)] = 1, \qquad [C_B(Q), F(B)_{p'}, P] \subseteq [F(B)_{p'}, P] = 1$$

であるから，3 部分群補題 5.8 により，

$$[P, C_B(Q), F(B)_{p'}] = 1$$

を得る．したがって (7.89) により

$$[P, C_B(Q)] \subseteq C_B(F(B)) \subseteq F(B) \qquad ([P, C_B(Q)]\subseteq C_B(Q) \text{ に注意})．$$

これは，$C_B(Q)$ が $PF(B)$ の上に作用することを示す．PQ は $PF(B)$ の S_p 部分群であるから，$C_B(Q)$ は PQ の上に作用し，$[PQ, C_B(Q)]\subseteq F(B)\cap PQ\subseteq Q$ である．x を $C_B(Q)$ の位数が p と素な元とすると，x の PQ への作用に対して補題 7.12 の (ii) を適用すれば，$[x, PQ]=1$, とくに $[x,P]=1$ を得る．▌

さてこれで定理 7.27 の証明を完成することができる．$[F(A)_{p'}, Q]=1$ であるから，$F(A)_{p'}\subseteq K$．(δ) と (7.88) を用いれば，

$$F(A)_{p'} \subseteq K \subseteq C_B(P) \subseteq N_B(P) \subseteq A.$$

よって，$F(A)_{p'}\subseteq F(K)_{p'}$ である．一方，$K\triangleleft B$ から，$F(K)_{p'}\subseteq F(B)_{p'}$．したがって $F(A)_{p'}\subseteq F(B)_{p'}$ を得る．A と B の対称性により $F(A)_{p'}=F(B)_{p'}$ でなければならない．ところで $|\pi(F(A))|\geqq 2$ と仮定しているから，$F(A)_{p'}=F(B)_{p'}\neq 1$．よって (7.88) により，$B=N_B(F(B)_{p'})=N_B(F(A)_{p'})\subseteq A$．したがって対称性により，$A=B$ となり矛盾である．▌

Bender はこの定理を巧みに運用することにより，Walter によって証明された‘可換 S_2 部分群をもつ有限単純群の分類定理’に非常に美しい証明を与えた．これを本書で述べるには，まだ多くの準備を必要とするので割愛せざるを得ない

が，興味のある読者は，H. Bender: On Groups with Abelian Sylow 2-Subgroups, Math. Z. **117** (1970), pp. 164-176, を参照されたい．以下で与える2信号関手定理の証明でも定理7.27が有効に用いられるであろう．そのとき，定理7.27の(ii)の場合に $A=B$ を示すために，ZJ 定理が用いられることを注意しておく．

さて，2信号関手定理の証明に入る前に，二つの補題を説明しなければならない．これらは，ともに思想的には§7.2, d)に属するものである．

補題 7.37 位数2の元 t が，奇数位数の可解群 X に作用しているとする．Y を X の $\langle t\rangle C_X(t)$ 不変な巾零部分群とするとき，$[t, Y]\subseteq F(X)$ である．

証明 奇素数 p に対して，$[t, O_p(Y)]\subseteq O_p(X)$ を示せばよいから，剰余群 $X/O_p(X)$ に移って考えれば，始めから $O_p(X)=1$ と仮定して $[t, O_p(Y)]=1$ を示せばよい．したがって $F=F(X)$ とおくと，F は p' 群で，Y は p 群であると仮定してよい．$U=C_F(Y)$ とおく．Y は $C_X(t)$ 不変だから，$[Y, C_F(t)]\subseteq Y\cap F=1$ となり，$C_F(t)\subseteq U$ である．よって定理7.5により t は $N_F(U)/U$ の上に固定点なしに作用する．このとき，補題7.18により，

$$\bar{x}^t=\bar{x}^{-1} \qquad (\forall \bar{x}\in N_F(U)/U)$$

であるから，$Y\ni y$ とすると，

$$\bar{x}^{[t,y]}=\bar{x}^{ty^{-1}ty}=(\bar{x}^{-1})^{y^{-1}ty}=(\bar{x}^{-y^{-1}})^{ty}=(\bar{x}^{y^{-1}})^{y}=\bar{x}$$

となり，$[t, Y]$ は $N_F(U)/U$ の上に自明な作用をする．ところで，$[t, Y, U]=1$ であるから，補題7.12の(ii)により $[t, Y]$ は $N_F(U)$ に自明に作用する．よって，$[t, Y]$ の F への作用に対して，補題7.12の(iv)を適用すれば，$[t, Y]$ は F に自明な作用をしなければならないことがわかる．よって $C_X(F)\subseteq F$ であるから，$[t, Y]\subseteq F$ を得る．ところで，$[t, Y]$ は p 群，F は p' 群であるから，$[t, Y]=1$ でなければならない．▌

補題 7.38 A を $m(A)\geqq 2$ なる Abel 群，X は A と位数が互いに素な可解群で，A は X に作用しているものとする．このとき，A の部分群 $T(\neq 1)$ に対して，

$$[T, X]=\langle [T, C_X(a)]\mid a\in A^{\sharp}\rangle$$

である．

証明 X を最小位数の反例とする．

(α) $[T, X] = X$.

$[T, X]=X_1$ とおくと，定理 7.5 の系により $[T, X_1]=X_1$ である．$X_1 \neq X$ とすると，X の最小性により，$[T, X_1]=X_1=\langle [T, C_{X_1}(a)] \mid a \in A^\sharp \rangle$．一方，$[T, C_{X_1}(a)] \subseteq [T, C_X(a)] \subseteq C_{X_1}(a)$ および定理 7.5 の系により，$[T, C_{X_1}(a)]=[T, C_X(a)]$．したがって，$[T, X]=X_1=\langle [T, C_X(a)] \mid a \in A^\sharp \rangle$ となり矛盾である．よって $X=X_1$.

(β) X は Abel 群である．

X は非可換群であるとしよう．X の極小な A 不変正規部分群を N とする．N は可換群だから，$X \neq N$ である．$\bar{X}=X/N$ とおくと，$|\bar{X}|<|X|$ より

$$\bar{X} = [T, \bar{X}] = \langle [T, C_{\bar{X}}(a)] \mid a \in A^\sharp \rangle = \langle \overline{[T, C_X(a)]} \mid a \in A^\sharp \rangle.$$

$X_0=\langle [T, C_X(a)] \mid a \in A^\sharp \rangle$ とおくと，$X=X_0N$ である．よって $X_0 \cap N$ は X の A 不変正規部分群 (N の可換性に注意) であるから，N の極小性により $X_0 \cap N =1$ または $X_0 \supseteq N$. $X_0 \supseteq N$ ならば $X=X_0$ となり矛盾．よって $X_0 \cap N=1$．このとき，$X \neq N$ より，$[T, N]=\langle [T, C_N(a)] \mid a \in A^\sharp \rangle \subseteq X_0$ となるから，$[T, N] \subseteq N \cap X_0=1$．このとき，

$$X = [T, X] = [T, X_0N] = [T, X_0] = X_0$$

となり矛盾である．

(γ) $A^\sharp \ni a$ に対して，$C_X(a)$ は T 不変であるから，定理 7.5 の系により，

$$C_X(a) = (C_X(a) \cap C_X(T))[T, C_X(a)]$$

である．これと定理 7.7 から，

$$\begin{aligned} X &= \langle C_X(a) \mid a \in A^\sharp \rangle \\ &= \langle C_X(a) \cap C_X(T), [T, C_X(a)] \mid a \in A^\sharp \rangle \\ &= \langle C_X(T), [T, C_X(a)] \mid a \in A^\sharp \rangle \\ &= \langle C_X(T), X_0 \rangle. \end{aligned}$$

(β) により X は可換群だから，$X=C_X(T)X_0$．このとき，

$$X = [T, X] = [T, C_X(T)X_0] = [T, X_0] = X_0$$

となり矛盾である．▌

定理 7.28 (Goldschmidt) G を有限群，A を $m(A) \geqq 3$ なる G の可換 2 部分群，

$$\theta: \ a \longmapsto \theta(C_G(a)) \qquad (a \in A^\sharp)$$

を G の A 信号関手すなわち

(i) $\theta(C_G(a))$ は $C_G(a)$ の A 不変な奇数位数の可解部分群,

(ii) $\theta(C_G(a))\cap C_G(b)\subseteqq\theta(C_G(b))$ $(\forall a, b\in A^{\sharp})$

とする．$\theta(G)=\langle\theta(C_G(a))\,|\,a\in A^{\sharp}\rangle$ とおくとき,

(7.91) $\theta(G)$ は奇数位数の可解群 で $C_{\theta(G)}(a)=\theta(C_G(a))$ $(\forall a\in A^{\sharp})$

である．——

$И_\theta(A)$ によって可解な θ 部分群全体の集合を表わす:

$$И_\theta(A)\ni X \Longleftrightarrow X=A\text{ 不変な奇数位数の可解部分群で,}$$
$$C_X(a)\subseteqq\theta(C_G(a))\quad(\forall a\in A^{\sharp})$$

である．2信号関手定理の結論 (7.91) は

$$И_\theta(A)\ni\theta(G)=\langle\theta(C_G(a))\,|\,\forall a\in A^{\sharp}\rangle$$

と同値である．また，$И_\theta{}^*(A)$ によって $И_\theta(A)$ の極大元全体の集合を表わす．さらに

$$\pi(\theta)=\bigcup_{a\in A^{\sharp}}\pi(\theta(C_G(a)))$$

とおく．ここで $\pi(\theta(C_G(a)))$ は $|\theta(C_G(a))|$ を割る素数全体の集合である．

さて，2信号関手定理の証明を始めよう．

定理 7.28 の証明 G を最小位数の反例として，θ を (7.91) が成立しない G の A 信号関手で $|\pi(\theta)|$ が最小なるものをとる．段階に分けて G の性質を調べて矛盾を導くであろう．

(α) H を $G\supsetneqq H\supseteqq A$ なる G の部分群とするとき，H に含まれる $И_\theta(A)$ の元で最大なものが存在する．このような $И_\theta(A)$ の元を，以後 $\theta(H)$ で表わす．

[証明] $$\theta_H(C_H(a))=\theta(C_G(a))\cap H\qquad(a\in A^{\sharp})$$

とおくと，θ_H は H の A 信号関手である．$X=\langle\theta_H(C_H(a))\,|\,a\in A^{\sharp}\rangle$ とおくと，$|H|<|G|$ より

$$X\text{ は奇数位数の可解群 で }C_X(a)=\theta_H(C_H(a))$$

である．とくに $X\in И_\theta(A)$ である．$Y\in И_\theta(A)$, $Y\subseteqq H$ とすると,

$$C_Y(a)\subseteqq\theta(C_G(a))\cap H=\theta_H(C_H(a))\qquad(\forall a\in A^{\sharp})$$

であるから，$Y=\langle C_Y(a)\,|\,a\in A^{\sharp}\rangle\subseteqq X$．したがって X が H に含まれる $И_\theta(A)$ の最大元である．▌

(β) $\mathcal{U}_\theta(A) \ni X \neq 1$ ならば，$G \neq N_G(X)$．とくに，$\mathcal{U}_\theta(A) \ni X \neq 1$ に対して $\theta(N_G(X))$ が定義される．また $\mathcal{M} = \mathcal{U}_\theta^*(A)$ とすると，$\mathcal{M}$ は Bender の定理の仮定 (7.88) を満たす．

[証明] $G = N_G(X)$ $(1 \neq X \in \mathcal{U}_\theta(A))$ と仮定して矛盾を導こう．$\bar{G} = G/X$ とおく．

$$\bar{\theta}(C_{\bar{G}}(\bar{a})) = \overline{\theta(C_G(a))} \qquad (a \in A^\sharp)$$

とすると，$\bar{\theta}$ は $\bar{G}$ の A 信号関手である．実際，$H = \theta(C_G(a))$ とすると，定理 7.5 により $C_{\bar{H}}(\bar{a}) = \overline{C_H(a)}$ $(a \in A^\sharp)$ であるから

$$\overline{\theta(C_G(b))} \supseteqq \overline{\theta(C_G(a)) \cap C_G(b)} = \overline{C_H(b)} = C_{\bar{H}}(\bar{b}) = \overline{\theta(C_G(a))} \cap C_{\bar{G}}(\bar{b})$$

である．したがって $|\bar{G}| < |G|$ より，$\bar{L} = \langle \overline{\theta(C_G(a))} \mid a \in A^\sharp \rangle$ は奇数位数の可解群で $C_{\bar{L}}(\bar{a}) \subseteqq \overline{\theta(C_G(a))}$ である．このとき，$L = \langle \theta(C_G(a)) \mid a \in A^\sharp \rangle$ も奇数位数の可解群となり，$C_L(a) \subseteqq \theta(C_G(a))X$ であるから $C_L(a) \subseteqq \theta(C_G(a))C_X(a) = \theta(C_G(a))$，よって $L \in \mathcal{U}_\theta(A)$．これは，$G$ が反例であることに反する．$\mathcal{M} = \mathcal{U}_\theta^*(A) \ni X, Y$，$Z$ を X の特性部分群 $(\neq 1)$ としよう．このとき，$N_Y(Z)$ は A 不変部分群であるから θ 部分群となり，(α) により，$N_Y(Z) \subseteqq \theta(N_G(Z)) = X$，すなわち (7.88) が成り立つ．▌

(γ) 各奇素数 p に対して，$\theta(C_G(A))$ 不変かつ位数が p と素な $\mathcal{U}_\theta(A)$ の元で最大なものが存在する．

[証明] $\theta(C_G(a))$ $(a \in A^\sharp)$ は A 不変な可解群であるから，問 7.11 の (iii) により $\theta(C_G(a))$ の $C_G(A) \cap \theta(C_G(a))$ 不変な p' 部分群で最大なものが存在する．それを $\theta_{p'}(C_G(a))$ と書く．$\theta(C_G(A)) = C_G(A) \cap \theta(C_G(a))$ $(\forall a \in A^\sharp)$ であるから，$\theta_{p'}(C_G(a))$ は $\theta(C_G(A))$ 不変である．このことから

$$a \longmapsto \theta_{p'}(C_G(a)) \qquad (a \in A^\sharp)$$

は G の A 信号関手であることが容易にわかる．ところで，$|\pi(\theta_{p'})| < |\pi(\theta)|$ であるから，$|\pi(\theta)|$ の最小性により，$K = \langle \theta_{p'}(C_G(a)) \mid a \in A^\sharp \rangle$ は奇数位数の可解群で $C_K(a) \subseteqq \theta_{p'}(C_G(a))$ である．$K = \langle C_K(a) \mid a \in A^\sharp \rangle$ (定理 7.7) と定理 7.6 の系から K は p' 部分群である．このとき，K が求めるものであることは容易に確かめられる．▌

(δ) $\mathcal{U}_\theta^*(A) \ni M \Longrightarrow C_A(M) = 1$.

[証明] $T_0 = C_A(M) \neq 1$ と仮定して矛盾を導く．$O_p(M) \neq 1$ なる素数 p をと

り，$O_p(M) \subseteq P \in И_\theta{}^*(A;p)$ とする．$N_P(O_p(M)) \subseteq \theta(N_G(O_p(M))) = M$ だから，$[N_P(O_p(M)), T_0]=1$．このとき，T_0 の P への作用に対して補題7.12の (iv) を用いて，$[P, T_0]=1$ を得る．すなわち $C_A(P) \neq 1$ である．$T=C_A(P)$ とおこう．このとき，

$$(7.92) \qquad И_\theta(A;p) \ni Q \Longrightarrow [T, Q]=1$$

が成り立つ．実際，可移性定理7.8により，$Q \subseteq P^* \in И_\theta{}^*(A;p)$ とすると，$P^x = P^*$ なる $x \in \theta(C_G(A))$ が存在し，$[T, Q] \subseteq [T, P^*] = [T, P^x] = [T, P]^x = 1$ である．つぎに

$$(7.93) \qquad \theta(C_G(A)) \subseteq H \in И_\theta(A) \Longrightarrow [T, H] \subseteq [T, K] \subseteq K$$

を示そう．ここで K は (γ) を満たす $И_\theta(A)$ の元である．$O_p(H \bmod O_{p'}(H)) = QO_{p'}(H)$，$Q=A$ 不変とすると，(7.92) により $[T, Q]=1$，すなわち $[T, O_p(H/O_{p'}(H))]=1$ である．このとき，T の $H/O_{p'}(H)$ への作用に対して補題7.12の (iii) を適用して，$[T, H/O_{p'}(H)]=1$，すなわち $[T, H] \subseteq O_{p'}(H)$ を得る．ところで，$H \supseteq \theta(C_G(A))$ であるから，$O_{p'}(H)$ は $\theta(C_G(A))$ 不変な $И_\theta(A)$ の元であり，よって (γ) により $O_{p'}(H) \subseteq K$ を得る．したがって $[T, H] \subseteq K$ であるが，定理7.5の系から $[T, H] \subseteq [T, K]$ を得る．これで，(7.93) が示された．$H = \theta(C_G(a))$ $(a \in A^\sharp)$ に (7.93) を適用すれば，$[T, \theta(C_G(a))] \subseteq C_K(a)$．定理7.5の系により

$$[T, \theta(C_G(a))] \subseteq [T, C_K(a)] \subseteq [T, \theta(C_G(a))]$$

となるから，

$$[T, \theta(C_G(a))] = [T, C_K(a)] \qquad (\forall a \in A^\sharp)$$

を得る．とくに

$$(7.94) \qquad [T, C_K(a)] \text{ は } \theta(C_G(T)) \cap C_G(a) = C_G(T) \cap \theta(C_G(a)) \text{ 不変}$$

である．$T \subseteq B \subseteq A$ なる非巡回部分群 B をとると，補題7.38により，$[T, K] = \langle [T, C_K(b)] \mid b \in B^\sharp \rangle$ であるから，(7.94) によって $[T, K]$ は $\theta(C_G(T)) \cap C_G(B)$ 不変である．ところで

$$\theta(C_G(T)) = \langle \theta(C_G(T)) \cap C_G(B) \mid m(A/B)=1,\ B \supseteq T \rangle \qquad (\text{定理7.7})$$

であるから，結局 $[T, K]$ は $\theta(C_G(T))$ 不変である．よって $M_0 = [T, K]\theta(C_G(T))$ とおくと，問7.9により $M_0 \in И_\theta(A)$ である．さて，$\theta(C_G(A)) \subseteq H \in И_\theta(A)$ としよう．定理7.5の系により $H = [H, T]C_H(T)$ であるが，(7.93) により $[H, T]$

$\subseteq[K, T]$. また $C_H(T)\subseteq\theta(C_G(T))$ であるから, $H\subseteq M_0$ を得る. とくに $H=\theta(C_G(a))$ とすると,

$$\theta(C_G(a)) \subseteq M_0 \qquad (\forall a \in A^{\sharp})$$

となり, $\theta(G)=\langle\theta(C_G(a))\,|\,a\in A^{\sharp}\rangle\subseteq M_0\in И_\theta(A)$ すなわち $\theta(G)\in И_\theta(A)$ を得る. これは G が反例であることに反する. ▌

いままでの議論では, 素数 2 の性質を全然用いていない. しかし, 以下の議論では素数 2 の性質——補題 7.37 および ZJ 定理——を本質的に用いるであろう.

(ε) A の $m(B)\geqq 2$ なる部分群 B と $И_\theta(A)\ni X\neq 1$ でつぎの性質を満たすものが存在する:

(i) $[B, X]=1$,

(ii) $X\subseteq H\in И_\theta(A) \Longrightarrow X\subseteq F(H)$.

[証明] $A^{\sharp}\ni a$ をとる. $\theta(C_G(a))\subseteq M\in И_\theta{}^*(A)$ とすると, (δ) により $\theta(C_G(a))\neq M$ すなわち $[a, M]\neq 1$ である. このとき a の M への作用に対して補題 7.12 の (iii) を適用して, $[a, F(M)]\neq 1$. $F=F(M)$ とおくと, 定理 7.7 により

$$F=\langle C_F(B)\,|\,m(A/B)=1\rangle$$

であるから, $[a, C_F(B)]\neq 1$ なる B が存在する. このときこのような B と $X=[a, C_F(B)]$ が (i), (ii) を満たす. $m(B)\geqq 2$, $И_\theta(A)\ni X\neq 1$, $[B, X]=1$ なることは明らかである. (ii) が成り立つことを示そう. $X\subseteq H\in И_\theta(A)$ とすると, $H\cap F$ は H の $C_H(a)$ 不変巾零部分群だから, 補題 7.37 により, $[a, H\cap F]\subseteq F(H)$. よって $X\subseteq H\cap F$ より $[a, X]\subseteq[a, H\cap F]\subseteq F(H)$. ところで, 定理 7.5 の系により $[a, X]=X$ であるから, $X\subseteq F(H)$ を得る. ▌

(ζ) B, X を (ε) のようにとり, $\theta(N_G(X))\subseteq H\in И_\theta{}^*(A)$ とする. このとき, $\theta(C_G(b))\subseteq H$ $(\forall b\in B^{\sharp})$ である.

[証明] (δ) により, $B^{\sharp}$ の各元 b に対して $\theta(C_G(b))$ 不変な $U\in И_\theta(A)$ で, $[b, U]\neq 1$ なるものが存在する. 実際, $\theta(C_G(b))\subseteq M\in И_\theta{}^*(A)$ なる M がそのような U の一つである. このような U で極小なものの一つを U_b としよう. $\theta(N_G(U_b))\subseteq M_b\in И_\theta{}^*(A)$ とする. このとき,

$$\theta(C_G(b)) \subseteq M_b$$

である. 以下の証明の方針は, M_b と H が Bender の定理 7.27 の仮定を満たすことを示し, 定理 7.27 の (ii) の場合に ZJ 定理を適用して $M_b=H$ を示すことで

ある．$F_b=F(M_b)$ とおく．

このとき，つぎの (7.95), (7.96) が成り立つことを示そう：

(7.95) $$[b, U_b] = U_b \subseteqq F_b, \quad [U_b, X] = 1,$$

(7.96) $$U_b \subseteqq L \in \mathcal{V}_\theta(A) \Longrightarrow U_b \in F(L).$$

b の U_b への作用に補題7.12の (iii) を適用すれば，$[b, F(U_b)] \neq 1$ である．$F(U_b)$ は $\theta(C_G(b))$ 不変であるから，U_b の極小性により $U_b=F(U_b)$，すなわち U_b は巾零群である．また U_b の極小性と定理7.5の系により，$[b, U_b]=U_b$ である．U_b は M_b の $C_{M_b}(b)$ 不変な巾零部分群であるから，補題7.37により

$$U_b = [b, U_b] \subseteqq F_b$$

を得る．ところで，$C_{F_b}(b) \subseteqq \theta(C_G(b)) \subseteqq N_G(U_b)$ と定理5.1の (ii) から，$[C_{F_b}(b), U_b] \subsetneqq U_b$ を得るが，$[C_{F_b}(b), U_b]$ は $\theta(C_G(b))$ 不変だから，U_b の極小性により

$$[C_{F_b}(b), U_b, b] = 1$$

である．明らかに $[b, C_{F_b}(b), U_b]=1$ であるから，3部分群補題5.8により，

$$[U_b, C_{F_b}(b)] = [U_b, b, C_{F_b}(b)] = 1$$

を得る．一方，$X \subseteqq \theta(C_G(b)) \subseteqq M_b$ と (ε) から，$X \subseteqq C_{F_b}(b)$．よって $[X, U_b]=1$ を得る．これで (7.95) が示された．$U_b \subseteqq L \in \mathcal{V}_\theta(A)$ としよう．$U_b \subseteqq L \cap F_b$ で，$L \cap F_b$ は L の $C_L(b)$ 不変な巾零部分群だから，補題7.37により，$U_b=[b, U_b] \subseteqq [b, L \cap F_b] \subseteqq F(L)$，すなわち (7.96) が示された．$(\varepsilon)$, (7.95) と (7.96) から

(7.97) $$U_b \subseteqq F(H), \quad N_{F(H)}(U_b) \subseteqq M_b,$$

(7.98) $$X \subseteqq F_b = F(M_b), \quad N_{F_b}(X) \subseteqq H$$

である．ところで，$\mathcal{M}=\mathcal{V}_\theta{}^*(A)$ とおくと (β) により $\mathcal{M}$ は (7.88) を満たし，(7.97) と (7.98) は Bender の定理において，$A=M_b$, $B=H$, $S=N_{F_b}(X)$, $T=N_{F(H)}(U_b)$ として，その定理の仮定を満たすことを示している．(H, M_b は可解群だから，$E(H)=E(M_b)=1$ に注意.) したがって，$H=M_b$ を示すためには，$F(H), F_b$ はともに p 群(p は奇素数)であると仮定してよい．H, M_b の A 不変な S_p 部分群をそれぞれ P, Q としよう．H, M_b は奇数位数の可解群，よって例題7.10により p 安定群であるから，Glauberman の ZJ 定理により，

$$H \triangleright ZJ(P), \quad M_b \triangleright ZJ(Q)$$

を得る．このとき，H, M_b は $\mathcal{V}_\theta(A)$ の極大元であるから，

(7.99) $$H = \theta(N_G(ZJ(P))), \quad M_b = \theta(N_G(ZJ(Q)))$$

でなければならない．とくに，

$$(7.100)\qquad P\in \mathcal{U}_\theta{}^*(A;p),\qquad Q\in \mathcal{U}_\theta{}^*(A;p)$$

である．実際，$P\subseteq P^*\in \mathcal{U}_\theta{}^*(A;p)$ とすると，$N_{P^*}(ZJ(P))\subseteq N_{P^*}(P)$ と (7.99) より，$P\subseteq N_{P^*}(P)\subseteq H$. よって $P=N_{P^*}(P)$，すなわち $P=P^*$ である．同様に $Q\in \mathcal{U}_\theta{}^*(A;p)$ を得る．さて (7.100) と可移性定理 7.8 により，$P^x=Q$ なる $x\in\theta(C_G(A))$ が存在する．このとき，

$$H^x=\theta(N_G(ZJ(P^x)))=\theta(N_G(ZJ(Q)))=M_b\qquad(x\in\theta(C_G(A)))$$

を得る．しかるに $x\in\theta(C_G(A))\subseteq\theta(C_G(b))\subseteq M_b$ であるから，

$$H=M_b{}^{x^{-1}}=M_b$$

となる．したがって，$\theta(C_G(b))\subseteq H$ である．▌

(ζ) を用いて，2 信号関手定理の証明を完成させることができる．$L\in \mathcal{U}_\theta(A)$ としよう．定理 7.7 により

$$L=\langle C_L(b)\,|\,b\in B^\sharp\rangle$$

であるから，(ζ) を用いて

$$C_L(b)\subseteq\theta(C_G(b))\subseteq H\qquad(\forall b\in B^\sharp)$$

を得る．したがって，$L\subseteq H$ である．とくに $L=\theta(C_G(a))$ とすると，

$$\theta(C_G(a))\subseteq H\qquad(\forall a\in A^\sharp).$$

したがって $\theta(G)=\langle\theta(C_G(a))\,|\,a\in A^\sharp\rangle\subseteq H\in \mathcal{U}_\theta(A)$ すなわち $\theta(G)\in \mathcal{U}_\theta(A)$ となり矛盾である．これで 2 信号関手定理 7.28 の証明が完成した．▌

ここで，2 信号関手定理の有限単純群の分類問題への応用例を示そう．しかし，有限単純群の分類に関する何らかの結果を得るためには，殆どすべての場合に，つぎに説明する (もう一つの) Bender の定理が必要である．この定理は，鈴木通夫氏の或る種の 2 重可移群に関する深い研究の結果を一般化したものであり，それは Feit-Thompson の定理とともに現在の有限単純群論の基本定理となっているものである．しかし残念ながら，現状ではこれら二つの基本定理は，両者とも書物でとり上げることは困難 (殆ど不可能) である．本章で説明してきたいろいろな事柄は，むしろこれらの基本定理を円滑に応用するための補助手段でもあるのであるが，下で述べる例題 7.11 でその効果を理解して頂ければ幸いである．

Bender の定理　有限群 G がつぎの条件を満たす真の部分群 H——そのような H を G の**強く埋め込まれた部分群**という——をもつとする：

(α)　H は偶数位数,

(β)　H の単位群でない任意の2部分群 U に対して $N_G(U) \subseteqq H$.

このとき，つぎの(i), (ii)のいずれかが成り立つ:

(i)　G の S_2 部分群は巡回群か4元数型の群である,

(ii)　G はつぎのような正規列をもつ:

$$G \rhd G_1 \rhd G_2 \rhd 1,$$

$$G/G_1,\ G_2 \quad \text{は} \quad \text{奇数位数},$$

$$G_1/G_2 \simeq SL(2, 2^n),\ Sz(2^n) \quad \text{または} \quad PSU(3, 2^n) \qquad (n \geqq 2).$$

ここで $Sz(2^n)$ はいわゆる Suzuki 群, $PSU(3, 2^n)$ は有限体 F_{2^n} 上の3次元特殊ユニタリ群の中心による商群である. $Sz(2^n)$ の定義については, §7.2, e) で引用した伊藤昇氏の著書を, また $PSU(3, 2^n)$ については, 本選書の"2次形式"を参照されたい.

なお, この定理の例題7.11への応用のためには, 定理の結論に現われる有限単純群で可換な S_2 部分群をもつものは, $SL(2, 2^n)$ に限ることに注意すれば十分である.

例題 7.11 (Gorenstein)　G を可換な S_2 部分群 A をもった有限単純群で

(α)　$m(A) \geqq 3$,

(β)　$A^\#$ の任意の元 a に対して $C_G(a)$ は可解群

とする. このとき, $G \simeq SL(2, 2^n)$ $(n \geqq 3)$.

(逆に $SL(2, 2^n)$ が(α), (β)を満たすことは容易にわかる. 読者自ら確かめよ.)

証明　以下有限群 X に対して $O_{2'}(X)$ を簡単に $O(X)$ で表わそう:

$$O(X) = O_{2'}(X) = X \text{ の奇数位数の最大の正規部分群}.$$

まず, (β)と例7.3により $C_G(a)$ $(a \in A^\#)$ は2束縛である. よって補題7.30により, G の任意の2局所部分群は2束縛である. L を G の2局所部分群とすれば

$$L \rhd BO(L), \qquad B \in \mathrm{Syl}_2(L) \tag{7.101}$$

である. 実際, $\bar{L} = L/O(L)$ とおけば, $F^*(\bar{L}) = O_2(\bar{L})$ であるが, $C_{\bar{L}}(F^*(\bar{L})) \subseteqq F^*(\bar{L})$ と $\mathrm{Syl}_2(L) \ni B$ の可換性から, (7.101)を得る. また例題7.7により

$$A^\# \ni a \longmapsto O(C_G(a))$$

は G の A 信号関手であるから,

$$W = \langle O(C_G(a)) \mid a \in A^\# \rangle$$

とおくと，2 信号関手定理 7.28 によって

$$W \text{ は 奇数位数の可解群}$$

である．さらに，定理 7.21 により

$$W \text{ は } G \text{ の } A \text{ 不変な奇数位数の可解部分群で最大なもの}$$

であることがわかる．これから，W は $N_G(A)$ 不変，よって $N_G(A)W$ は G の部分群となる．$H=N_G(A)W$ とおく．H が G の強く埋め込まれた部分群であることを示そう．まず G は単純群であるから，明らかに $G\neq H$ である．つぎに，H の任意の 2 部分群 $U\neq 1$ に対して $N_G(U)\subseteq H$ を示さねばならないが，$A\in \mathrm{Syl}_2(H)$ であるから，$A\supseteq U$ と仮定しても一般性を失わない．このとき，$N_G(U)\supseteq A$，したがって $A\in \mathrm{Syl}_2(N_G(U))$ であるから，(7.101) を用いて

$$N_G(U) \triangleright AO(N_G(U))$$

である．したがって補題 7.1 の (ii) により

$$N_G(U) = (N_G(U)\cap N_G(A))O(N_G(U)) \subseteq N_G(A)O(N_G(U)). \tag{7.102}$$

しかるに，問 7.32 の (i) により $O(N_G(U))=O(C_G(U))$．a を U の任意の位数 2 の元とすると，$C_G(a)\supseteq C_G(U)$ であるから，補題 7.28 により，$O(C_G(a))\supseteq O(C_G(U))$ である．よって

$$W \supseteq O(C_G(a)) \supseteq O(N_G(U)) \tag{7.103}$$

を得る．(7.102), (7.103) から

$$N_G(U) \subseteq N_G(A)W = H$$

を得る．すなわち H は G の強く埋め込まれた部分群である．したがって Bender の定理により $G\simeq SL(2,2^n)$ である．∎

最後に例題 7.11 と Bender の定理に関していくつかの注意をして，この章を終りにしよう．

注意 (i) 例題 7.11 において $m(A)=2$ ならば，$G\simeq PSL(2,q)$ ($q\equiv 3$ または 5 (mod 8), $q\geqq 5$) であることが知られている (Gorenstein)．しかし，この証明は例題 7.11 に比べてかなり難しい．補助手段も本章で説明してきた事のほかに群指標の理論 (モジュラー表現を含めて) が必要である．このように，Sylow 部分群が‘小さい’とき，特別な扱いが必要になるというのは，有限単純群論に現われる一つの著しい現象である．

(ii) 上に述べた Bender の定理は，その主張が非常に特別な群に関係したものであるから，その応用範囲も一見狭いものであるかのように思えるが，実はそうではない．実際，有限群 G に関する或る命題 P を証明するときに，命題 P の真偽が，G が強く埋め込まれ

た部分群をもつ場合に帰着され，したがって Bender の定理に現われる特別な群に対して P の真偽を確かめることにより，P が証明できることがしばしば起るのである．たとえば，§7.4, a) の最後の方で言及した Gorenstein–Walter の定理が，その典型的な例である．この Gorenstein–Walter の定理も，2信号関手定理と Bender の定理の応用として証明されるのであり，それは実はそれ程難しくはない．意欲のある読者は，例題7.11を参考にしてその証明を試みられたい．

(iii)　強く埋め込まれた部分群をもつ有限群のやさしい性質については，§7.4, b) で引用した

D. Gorenstein： Finite Groups, Harper & Row (1968)

の第9章で解説されている．さらに，そこでは偶数位数の群の取り扱いの基本事項も述べられている．実は本書でも，このことを本章でとり上げるのが望ましかったと思うのであるが，都合上それについては第8章で説明するであろう．なお，本章で説明してきた事は上記 Gorenstein の著書と重複するところが多いが，本章ではその後の進展についてもふれてある．

(iv)　Bender の定理の証明に関心のある読者のために文献をあげておく．最初に§7.2 e) でも引用した

伊藤昇：有限群論，共立出版(1970)

を読まれることをおすすめする．この本は，前にも述べたように Zassenhaus 群の分類の完全な記述を目標としたものであるが，Bender の定理はその結果が土台になっているのである．ついで

M. Suzuki： On a class of doubly transitive groups II, Ann. of Math. **79** (1964), 514–589,

H. Bender： Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt, Journal of Algebra **17** (1971), 527–554

の2論文で Bender の定理が証明されている．

(v)　鈴木通夫氏による群論上，下が岩波書店より1977, 78年に刊行されている．そこでは本書で説明してきた事柄に加えて，より多くの話題がとり上げられている．たとえば，§7.3の移送定理についても本講ではふれなかった重要な結果が解説されており，また§7.4, b) では省略した Dickson の定理の証明も述べられている．最近の有限群論のより進んだ話題に興味のある方は，この鈴木氏の書物を是非お読みになることをおすすめする．

第8章　有限群の表現論

本章では有限群の表現論について解説する．最初に注意すべきことは，本章は必ずしも第7章に続くものではないということである．実際，§8.1–§8.6の理解のために必要なことは，(円体や有限体の Galois 群に関する簡単な事実もときどき用いるけれども）本書の第1–6章で解説した群論の常識と大学教養課程の線型代数である．ただし，有限群論への応用を述べる最後の2節§8.7–§8.8では，第7章から自由に引用するであろう．

本書では，主として複素数体上の表現を取り扱い，群指標およびその応用に重点をおいて解説した．したがって記述は古典的方法によるものを採用した．有限群の表現論を群環やその上の加群の言葉で記述するもっと環論的な方法もあり，それは理論上非常に重要であり，またより進んだ表現論にとっては不可欠のものである．しかし群指標の理論をなるべく早く，またその応用をなるべく多く，解説するにはそれが一番早道であるというのが，本書で古典的方法を採用した理由である．なお，各節の内容については，節の始めに概要を述べてあるので参照されたい．

§8.1　基本的概念

本節では，表現に関する基本的概念を説明する．a) では表現の定義と例について述べ，b) では部分表現，表現の和，積などについて説明する．c) では，群環と群環上の加群について後に必要な事柄の最小限の説明をする．最後に d) では，表現の完全可約性に関する Maschke の定理を述べる．なお，本節と次節では，一般の体の上の表現を扱っているが，§8.3以降では複素数体上の表現に限られるので，始めから体は複素数体と思って読んでも差支えはない．

a) 表現の定義と例

G を有限群，V を体 k 上の有限次元線型空間とする．G から一般線型群 $GL(V)$ への準同型写像 ρ が与えられたとき，ρ を G の V における**表現**，V を ρ の**表現空間**という．これらのことを簡単に G の k 上の表現 (ρ, V) といい表わすこともある．V の次元を表現 ρ の**次数**といい，$\deg\rho$ で表わす．また，ρ が単射のとき，(ρ, V) は**忠実**であるという．(ρ, V) が忠実であるためには，準同型 ρ の核すなわち $\mathrm{Ker}\,\rho=\{x\in G\mid \rho(x)=1_V\}$ (1_V は V の恒等変換）が単位群であることが必要十分である．

(ρ_1, V_1), (ρ_2, V_2) を G の体 k 上の表現としよう．V_1 から V_2 への (線型空間としての) 同型写像 f が存在して

$$f\circ\rho_1(x) = \rho_2(x)\circ f \qquad (\forall x \in G) \tag{8.1}$$

が成り立つとき，(ρ_1, V_1) と (ρ_2, V_2) は**同型**であるといい，

$$(\rho_1, V_1) \sim (\rho_2, V_2)$$

あるいは簡単に

$$\rho_1 \sim \rho_2$$

と書く．二つの表現の同型は，つぎの図式が可換であることを意味する．同型な二つの表現は本質的に同じものである．

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ {\scriptstyle\rho_1(x)}\downarrow & & \downarrow{\scriptstyle\rho_2(x)} \\ V_1 & \xrightarrow[f]{} & V_2 \end{array}$$

R が有限群 G から k 上の n 次一般線型群 $GL(n, k)$ への準同型であるとき，R を G の k 上の **n 次行列表現**という．R_1, R_2 を G の k 上の n 次行列表現とするとき，

$$SR_1(x) = R_2(x)S \qquad (\forall x \in G) \tag{8.2}$$

を満たす n 次正則行列 S が存在するならば，行列表現 R_1, R_2 は**同値**であるという．V として k の元を成分とする n 項列ベクトル全体からなる線型空間 k^n をとり，$GL(n, k)$ の元を k^n の線型変換とみるとき，k 上の n 次行列表現は最初に述べた意味で G の k 上の表現を与える．また，二つの行列表現の同値は，これらを G の数ベクトル空間 k^n における表現と見たとき，これら二つの表現が同型であることにほかならない．

G の k 上の表現 (ρ, V) に行列表現を対応させよう．$v_1, v_2, \cdots, v_n$ ($n=\deg\rho$) を V の基底とするとき，線型変換 $\rho(x)$ $(x \in G)$ に対して

$$\rho(x)v_j = \sum_{i=1}^{n} r_{ij}(x)v_i \qquad (j=1, 2, \cdots, n) \tag{8.3}$$

によって，$\rho(x)$ に対応する n 次行列

$$R(x) = (r_{ij}(x))$$

を定める．このとき，

$$R(xy)=R(x)R(y) \qquad (x, y \in G)$$

が成り立つことは容易に確かめられる．すなわち

$$G \ni x \longmapsto R(x) \in GL(n, k)$$

は，G の k 上の n 次行列表現である．このようにして得られた行列表現を (ρ, V) の**行列表現**あるいは**行列表示**という．V の異なる2組の基底をとるとき，二つの行列表現が得られるが，これらは同値である．実際，$\{v_1, v_2, \cdots, v_n\}$, $\{u_1, u_2, \cdots, u_n\}$ を V の2組の基底とするとき，

$$u_j=\sum_{i=1}^{n} s_{ij}v_i \qquad (j=1, 2, \cdots, n)$$

によって，n 次行列 $S=(s_{ij})$ を定めれば，S が(8.2)を満たす．

また，(ρ_1, V_1), (ρ_2, V_2) が G の同型な表現であるためには，それぞれの行列表示が同値であることが必要十分である．

問 8.1 このことを確かめよ．——

以上により，有限群 G の表現を与えることと，行列表現を与えることは，本質的に同じことであることがわかる．したがって，以後有限群 G の表現を行列表現の形で与えることもあるであろう．

例 8.1 1次表現とくに恒等表現 (ρ, V) を G の体 k 上の表現とする．$\dim_k V=1$ すなわち $\deg\rho=1$ のとき，(ρ, V) を G の k 上の**1次表現**という．(ρ, V) の行列表示を考えると，1次表現には G から体 k の乗法群 k^* への準同型が対応し，同型でない二つの1次表現には，G から k^* への異なる準同型が対応する．

n 次対称群 $\mathfrak{S}_n$ の元 σ にその符号 $\mathrm{sgn}(\sigma)$ ((1.7), p.8参照)を対応させると，これは $\mathfrak{S}_n$ から複素数体の乗法群 $\boldsymbol{C}^*$ への準同型であるから，$\mathfrak{S}_n$ の $\boldsymbol{C}$ 上の1次表現が得られる．これを $\mathfrak{S}_n$ の**交代表現**という．

G を位数 n の巡回群，a をその生成元，ω を1の原始 n 乗根(たとえば $\omega=\cos(2\pi/n)+\sqrt{-1}\sin(2\pi/n)$)，$i$ を任意の整数とするとき，

$$\rho_i(a^k)=\omega^{ik} \qquad (k=0, 1, \cdots, n-1)$$

によって，G の $\boldsymbol{C}$ 上の1次表現 ρ_i が得られる．もちろん $i\equiv j \pmod n$ のとき，$\rho_i=\rho_j$ である．

一般に V を k 上の1次元線型空間とするとき，有限群 G の各元 x に V の恒等変換を対応させれば，これは G の k 上の1次表現を与える．このような表現

を**恒等表現**といい，1_G で表わす．恒等表現は，表現としてはまことにつまらないものであるが，表現論において無視することはできない．

例 8.2　置換表現　有限群 G が n 個の元からなる集合 Ω の上に（左から）作用しているとする．簡単のために

$$\Omega=\{1, 2, \cdots, n\}$$

とする．V を体 k 上の n 次元線型空間，$v_1, v_2, \cdots, v_n$ をその基底とする．$G\ni\sigma$ に対して

$$\rho(\sigma)v_j=v_{\sigma(j)}$$

によって，V の線型変換 $\rho(\sigma)$ が定まる．このとき，

$$\sigma\longmapsto\rho(\sigma)$$

は G から $GL(V)$ への準同型であり，したがって G の表現 (ρ, V) が定まる．このような表現を G の**置換表現**という．$G\ni\sigma$ に対して

$$P_{ij}(\sigma)=\begin{cases}1 & (i=\sigma(j)),\\ 0 & (i\neq\sigma(j))\end{cases}$$

とおき，n 次行列 $P(\sigma)=(P_{ij}(\sigma))$ を作れば

$$\sigma\longmapsto P(\sigma)$$

が，置換表現 P の行列表示である．$P(\sigma)$ は各行各列に 1 がただ 1 回現われる行列である．このような行列を**置換行列**という．H を G の部分群として，

$$G=x_1H+x_2H+\cdots+x_nH$$

を G の H による左剰余類への分解としよう．G は G/H の上に

$$x\circ x_iH=xx_iH \qquad (x\in G)$$

によって作用する（例 2.2, p. 55）．したがって上のようにして G の置換表現が得られる．このような置換表現を $1_H{}^G$ で表わす．同様にして

$$G=Hx_1+Hx_2+\cdots+Hx_n$$

を G の H による右剰余類への分解とするとき，

$$x\circ Hx_i=Hx_ix^{-1} \qquad (x\in G)$$

によって G は $H\backslash G$ に作用するから，G の置換表現が得られる．このとき，

$$G=x_1{}^{-1}H+\cdots+x_n{}^{-1}H,$$

$$Hx_ix^{-1}=Hx_j \Longleftrightarrow xx_i{}^{-1}H=x_j{}^{-1}H$$

であるから，この置換表現は上で定義した $1_H{}^G$ と同型であることがわかる（対応

する行列表示が全く同一にとれることに注意). したがってこの置換表現もやはり $1_H{}^G$ で表わされる. 置換表現 $1_H{}^G$ において, とくに H が単位群のときこの表現を G の**正則表現**といい, 簡単に 1^G で表わす.

注意 ここで定義した置換表現 $1_H{}^G$ は, §8.4 で説明される誘導表現の特別な場合である. すなわち H の恒等表現から誘導された G の表現が $1_H{}^G$ にほかならない.

問 8.2 G を $\{1, 2, 3\}$ の上の3次対称群, $H=\langle(1\ 2)\rangle$ すなわち互換 $(1\ 2)$ で生成される部分群とするとき, 置換表現 $1_H{}^G$ に対応する行列表現を求めよ.

例 8.3 正2面体群の表現 D_{2n} を位数 $2n$ の正2面体群としよう (例1.13, p.30). a を正 n 角形の中心のまわりの角 $2\pi/n$ の回転, b を正 n 角形の或る対称軸に関する折返しとすると, a, b は D_{2n} の生成系であり

$$a^n = b^2 = 1, \quad b^{-1}ab = a^{-1} \tag{8.4}$$

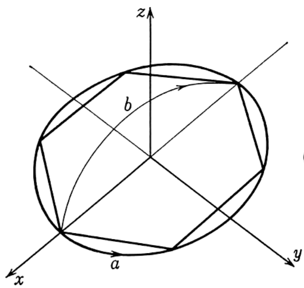


図5

が, その基本関係である. a, b を, 座標系を適当に定めた3次元 Euclid 空間における行列で表示すると,

$$a \longmapsto \begin{bmatrix} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} & \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} & \\ & & 1 \end{bmatrix},$$

$$b \longmapsto \begin{bmatrix} -1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

となり，これから D_{2n} の $\boldsymbol{C}$ 上の3次表現が得られる．これらの行列の形から，

$$a \longmapsto \begin{bmatrix} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} \end{bmatrix}, \tag{8.5}$$

$$b \longmapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

なる対応によって D_{2n} の2次表現が得られることは明らかであろう．さて任意の整数 l に対して D_{2n} の2次表現 R_l を与えよう：

$$R_l(a) = \begin{bmatrix} \cos\dfrac{2\pi l}{n} & -\sin\dfrac{2\pi l}{n} \\ \sin\dfrac{2\pi l}{n} & \cos\dfrac{2\pi l}{n} \end{bmatrix},$$

$$R_l(b) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

とおくと，R_l は D_{2n} の2次表現を与える．このことを見るには，(8.4) が D_{2n} の生成系 a, b の基本関係であるから，対応する行列 $R_l(a), R_l(b)$ が (8.4) と同じ関係

$$R_l(a)^n = R_l(b)^2 = 1, \qquad R_l(b)^{-1}R_l(a)R_l(b) = R_l(a)^{-1}$$

を満たすことを確かめれば十分である．これは行列の直接の計算によって確かめられる．なお，明らかに

$$l \equiv l' \pmod{n} \Longrightarrow R_l = R_{l'}$$

である．同様にして $\omega = \cos(2\pi/n) + \sqrt{-1}\sin(2\pi/n)$ とするとき，

$$R_l'(a) = \begin{bmatrix} \omega^l & 0 \\ 0 & \omega^{-l} \end{bmatrix}, \qquad R_l'(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

によって，D_{2n} の2次表現 R_l' が得られる．R_l は行列の成分が実数であるから，D_{2n} の実数体上の2次表現であるが，これを複素数体上の表現と考えれば，R_l' と同値な表現である．実際，$S = \begin{bmatrix} 1 & \sqrt{-1} \\ -1 & \sqrt{-1} \end{bmatrix}$ とおくと，

$$SR_l(a) = R_l'(a)S, \qquad SR_l(b) = R_l'(b)S$$

が行列の計算によって確かめられる．なお，

$$l \equiv -l' \pmod{n} \Longrightarrow R_l \sim R_{l'}$$

である．このことを見るには，上のように(8.2)を満たす S を直接に求めて確かめることもできるが，後に説明するように R_l と $R_{l'}$ の指標の一致を見る方がより簡単である．

例 8.4　4元数型の群の表現

$$a^{2n}=1, \qquad a^n=b^2, \qquad b^{-1}ab=a^{-1}$$

を基本関係とする群 Q_{4n} を4元数型の群というのであった(例1.14, p.31)．$\omega=\cos(\pi/n)+\sqrt{-1}\sin(\pi/n)$ とするとき，

$$Q_l(a)=\begin{bmatrix}\omega^l & 0\\ 0 & \omega^{-l}\end{bmatrix}, \qquad Q_l(b)=\begin{bmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{bmatrix}^l$$

によって，各整数 l に対して，4元数型の群 Q_{4n} の2次表現が得られることが，D_{2n} の場合と全く同様にしてわかる．

b）部分表現，表現の和，表現の積

ここでは，あらかじめ与えられたいくつかの表現から他の表現を構成することを述べる．

(α)　**部分表現と商表現**

(ρ, V) を G の体 k 上の表現とする．V の部分空間 W が

$$\rho(x)W\subseteq W \qquad (\forall x\in G)$$

なる条件を満たすとき，W は ρ **不変**であるといわれる．W を ρ 不変な V の部分空間とするとき，V の線型変換 $\rho(x)$ を W に制限した線型変換を $\rho_W(x)$ と書くと

$$x\longmapsto \rho_W(x) \qquad (x\in G)$$

は，G の W における表現である．このような表現 (ρ_W, W) を (ρ, V) の**部分表現**という．これを行列表現についていうと，G の行列表現 R が，

$$R(x)=\begin{bmatrix}R_1(x) & *\\ 0 & R_2(x)\end{bmatrix} \tag{8.6}$$

$$(R_1(x), R_2(x) \text{は一定次数の正方行列})$$

なる形をしているとき，

$$x\longmapsto R_1(x) \qquad (x\in G)$$

は G の行列表現を与え，これが R の部分表現である．実際，$\begin{bmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ $\left.\begin{matrix} \\ \\ \\ \end{matrix}\right\}k$ (k は R_1 の次数) なる数ベクトル全体の作る部分空間 W が R 不変な部分空間であり，R の W への制限が R_1 である．また，W が V の ρ 不変部分空間であるとき，V の線型変換 $\rho(x)$ は商空間 V/W の線型変換 $\rho_{V/W}(x)$ を誘導し，

$$x \longmapsto \rho_{V/W}(x)$$

は，G の V/W における表現を与える．このような表現 $(\rho_{V/W}, V/W)$ を (ρ, V) の (W による) **商表現**という．これを行列表現についていえば，行列表現 R が (8.6) の形をしているとき，

$$x \longmapsto R_2(x)$$

が，行列表現 R の商表現を与える．

注意　G の表現 (ρ, V) が完全可約 (§8.1, d) 参照) のとき，部分表現と商表現を区別する必要はない．本書では，主として複素数体上の表現を取り扱い，そのような表現はつねに完全可約 (定理 8.1) だから，本書では商表現を本質的に用いることはない．

(β)　表現の和

(ρ_1, V_1), (ρ_2, V_2) をそれぞれ G の k 上の表現とする．V を V_1 と V_2 の直和 $V_1 \oplus V_2$ とすると，$G \ni x$,　$V \ni v = v_1 + v_2$ $(v_i \in V_i)$ に対して

$$\rho(x)v = \rho_1(x)v_1 + \rho_2(x)v_2$$

とおいて，G の V における表現が得られる．このような表現を ρ_1 と ρ_2 の**和** (あるいは**直和**) とよび，

$$\rho = \rho_1 \oplus \rho_2$$

と書く．V_1, V_2 のそれぞれに基底をとり，ρ_1, ρ_2 の行列表示をそれぞれ $R_1(x)$, $R_2(x)$ とすれば，ρ の行列表示は

$$x \longmapsto \begin{bmatrix} R_1(x) & 0 \\ 0 & R_2(x) \end{bmatrix} \qquad (x \in G)$$

となる．逆に G の表現 (ρ, V) が与えられたとき，V が ρ 不変部分空間 V_1, V_2 の直和ならば，(ρ, V) は部分表現 (ρ_{V_1}, V_1) と (ρ_{V_2}, V_2) の和と同型である．

例 8.5　有限群 G が有限集合 Ω に作用しているとき，これから得られる置換

表現を ρ としよう．$\Omega_1, \Omega_2, \cdots, \Omega_t$ を (G, Ω) のすべての軌道とするとき，G の Ω_i への作用から置換表現 ρ_i $(1 \leqq i \leqq t)$ が得られる．このとき ρ の構成の仕方から，ρ は $\rho_1, \rho_2, \cdots, \rho_t$ の直和であることがわかる．

(γ) 表現の積

$(\rho_1, V_1), (\rho_2, V_2)$ を G の k 上の表現とする．$V_1 \otimes V_2$ を線型空間 V_1, V_2 のテンソル積，$x \in G$ に対して $\rho_1(x) \otimes \rho_2(x)$ を線型変換のテンソル積とするとき，

$$x \longmapsto \rho_1(x) \otimes \rho_2(x)$$

は，G の $V_1 \otimes V_2$ における表現を与える．このような表現を $(\rho_1, V_1), (\rho_2, V_2)$ の**テンソル積**あるいは簡単に**積**といい，$(\rho_1 \otimes \rho_2, V_1 \otimes V_2)$ で表わす．

注意 ここでは，一応テンソル積の概念は既知とするが，§8.4, d) においてもう少し一般のテンソル積の概念を説明してあるので参照されたい(とくに例 8.16 において線型空間のテンソル積を説明してある)．なお §8.4, d) は直ちに読むことができる．

表現のテンソル積に対応する行列表現を調べよう．まず m 次行列 $A=(a_{ij})$ および n 次行列 B に対して

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}$$

によって mn 次正方行列 $A \otimes B$ を定義する．$A \otimes B$ を A, B の **Kronecker 積**とよぶことがある．さて，V_1 の基底 $v_1, v_2, \cdots, v_m$，V_2 の基底 $u_1, u_2, \cdots, u_n$ をとれば，

$$v_1 \otimes u_1, \quad \cdots, \quad v_1 \otimes u_n, \quad \cdots, \quad v_m \otimes u_1, \quad \cdots, \quad v_m \otimes u_n$$

が $V_1 \otimes V_2$ の基底である．$R_1(x), R_2(x)$ をそれぞれ(基底 $\{v_i\}$, $\{u_j\}$ を用いて作った)$(\rho_1, V_1), (\rho_2, V_2)$ の行列表現とすると，$V_1 \otimes V_2$ の上の基底に関する行列表現は

$$x \longmapsto R_1(x) \otimes R_2(x)$$

であることが，(8.3) に従って計算すればわかる．

c) 群環の表現と群環上の加群

k を体，$k[G]$ を有限群 G の k 上の群環とする．$k[G]$ は形式和

$$\sum_{x \in G} a_x x \qquad (a_x \in k)$$

全体の集合であり，

$$\sum_{x \in G} a_x x + \sum_{x \in G} b_x x = \sum_{x \in G} (a_x + b_x) x,$$

$$\left(\sum_{x\in G}a_x x\right)\left(\sum_{x\in G}b_x x\right)=\sum_x\left(\sum_y a_y b_{y^{-1}x}\right)x$$

なる和と積に関して環である．さらに G の位数を n とすれば，$k[G]$ は k 上の n 次元線型空間でもある．また G は自然に $k[G]$ の部分集合と考えることができる．すなわち $G\ni g$ を

$$a_x=\begin{cases}1 & (x=g),\\ 0 & (x\neq g)\end{cases}$$

なる $k[G]$ の元 $\sum_{x\in G}a_x x$ と同一視するのである．このとき，$k[G]$ における積の定義からわかるように，G は環 $k[G]$ の乗法群の部分群である．

$$Z(k[G])=\{z\in k[G]\mid xz=zx\ (\forall x\in G)\}$$

とおく．明らかに $Z(k[G])$ は $k[G]$ の可換部分環である．$Z(k[G])$ を $k[G]$ の**中心**という．$k[G]\ni z=\sum_{x\in G}a_x x$ において

(8.7)　　$z\in Z(k[G]) \iff x, x'$ が共役のとき $a_x=a_{x'}$

であることは，$Z(k[G])$ の定義から明らかであろう．$K_1, K_2, \cdots, K_h$ を G の共役類の全体とするとき，

$$\hat{K}_i=\sum_{x\in K_i}x \qquad (i=1,2,\cdots,h)$$

なる $k[G]$ の元 $\hat{K}_1, \hat{K}_2, \cdots, \hat{K}_h$ は中心 $Z(k[G])$ の基底をなすことが，(8.7) からわかる．したがって $Z(k[G])$ は $k[G]$ の h 次元部分空間である．また，$\hat{K}_i, \hat{K}_j$ の積を $\hat{K}_1, \cdots, \hat{K}_h$ の線型結合

$$\hat{K}_i\hat{K}_j=\sum_{k=1}^{h}a_{ijk}\hat{K}_k \qquad (a_{ijk}\in k)$$

として表わせば，a_{ijk} は負でない整数（を k の元と考えたもの）である．実際，a_{ijk} は $K_k\ni x_k$ を固定するとき，$xy=x_k$ $(x\in K_i,\ y\in K_j)$ なる (x, y) の組の数に等しい．

例 8.6　正則表現の表現空間　有限群 G の群環 $k[G]$ 上の表現 ρ をつぎのように作ることができる．すなわち

$$\rho(x)\left(\sum_{y\in G}a_y y\right)=\sum_{y\in G}a_y xy=\sum_y a_{x^{-1}y}y$$

によって，$k[G]$ 上の線型変換 $\rho(x)$ を定義すると，G の $k[G]$ における表現が

得られる．この表現は，例 8.2 で述べた正則表現にほかならないことは容易にわかる．——

群環の表現 (ρ, V) を G の k 上の表現とする．$k[G]\ni h=\sum a_x x$ に対して

$$\rho(h) = \sum a_x \rho(x)$$

によって，V の線型変換 $\rho(h)$ $(h\in k[G])$ を定義すれば，

$$h \longmapsto \rho(h)$$

なる $k[G]$ から $\mathrm{End}(V)$ への写像は，$k[G]$ から $\mathrm{End}(V)$ への k **準同型**——環としての準同型でしかも k 上の線型写像——であることが容易に確かめられる．すなわち群 G の k 上の表現から，群環の k 上の表現が自然に得られるわけである．逆に ρ を $k[G]$ の V における表現すなわち $k[G]$ から $\mathrm{End}(V)$ への k 準同型とするとき，$G\subseteqq k[G]$ と考えれば，

$$x \longmapsto \rho(x) \qquad (x\in G)$$

は，G の V における表現を与える．したがって，群の k 上の表現を与えることと，群環の k 上の表現を与えることは同じことである．

$k[G]$ 加群 V を左 $k[G]$ 加群としよう（環上の加群の概念は，§3.5, p.91 参照）．まず，V は k 上の線型空間であることに注意する．すなわち，$k\ni\alpha$，$V\ni v$ に対して α と v のスカラー積を

$$\alpha v = (\alpha 1)v$$

によって定義するのである．右辺において $\alpha 1$（1 は G の単位元）は $k[G]$ の元，積 $(\alpha 1)v$ は $k[G]$ 加群としての積である．このとき，左 $k[G]$ 加群 V から，G の V における表現がつぎのようにして得られる．$V\ni v$，$G\ni x$ に対して

$$v \longmapsto xv$$

なる対応は，V の k 上の線型変換である．これを $\rho(x)$ で表わせば

$$x \longmapsto \rho(x)$$

は，G から $GL(V)$ への準同型であり，したがって G の表現を与えることは容易に確かめられる．逆に (ρ, V) を G の k 上の表現としよう．(ρ, V) を群環 $k[G]$ の表現に拡張し，

$$\left(\sum a_x x\right)v = \rho\left(\sum a_x x\right)v \qquad (v\in V)$$

によって，$k[G]$ の元と V の元の積を定義すれば，V は左 $k[G]$ 加群となる．さらにこの左 $k[G]$ 加群から，上のようにして得られる G の表現は，(ρ, V) に

ほかならない.

以上まとめると,

G の k 上の表現を与えること,

群環 $k[G]$ の表現を与えること,

左 $k[G]$ 加群を与えること

が, すべてまったく同じことであることがわかる. 理論上, 群の表現を群環の表現に拡張して考えたり, 左 $k[G]$ 加群の言葉で群の表現論を記述したりするのが便利であることがしばしば起るので, 本講でもときどきこのような記述をするであろう.

問 8.3 V_1, V_2 を左 $k[G]$ 加群, $(\rho_1, V_1), (\rho_2, V_2)$ をそれぞれ V_1, V_2 から得られる G の表現とするとき, V_1, V_2 が左 $k[G]$ 加群として同型であることと, $(\rho_1, V_1), (\rho_2, V_2)$ が同型であることは同値であることを確かめよ.

d) Maschke の定理

(ρ, V) を有限群 G の体 k 上の表現としよう. G の ρ 不変な部分空間が自明なもの——V 自身および零ベクトルのみからなる部分空間 $\{0\}$ ——に限るとき, (ρ, V) は k 上**既約**であるといわれる. 既約でないとき, **可約**という.

問 8.4 G の Ω への作用から得られる置換表現は $|\Omega|>1$ ならばつねに可約である. もっと詳しく, 置換表現は恒等表現を部分表現として含むことを示せ. ——

また (ρ, V) が, いくつかの既約表現 (ρ_i, V_i) $(i=1, 2, \cdots, l)$ の直和と同型であるとき, (ρ, V) は**完全可約**であるという. 有限群の表現は, つねに完全可約であるとは限らないが, 完全可約であるための十分条件として, §7.1 で述べた Maschke の定理 (例題 7.1, p. 154) は有名である. この定理は非常に大切な定理なので, 読者の便利のためこの定理と証明をここでも述べておこう.

定理 8.1 (Maschke) (ρ, V) を有限群 G の体 k 上の表現とする. k の標数が G の位数を割らないならば, (ρ, V) は完全可約である. とくに標数 0 の体の上の表現は完全可約である.

証明 つぎのことを証明すればよい:

(*) V_1 を V の ρ 不変部分空間とするとき,

$$V = V_1 \oplus V_2 \quad (\text{直和})$$

なる ρ 不変部分空間 V_2 が存在する.

この命題(*)が証明されれば，定理 8.1 を V の次元に関する帰納法で証明することにすれば，$V_1(\neq 0)$, V_2 は完全可約すなわちそれぞれが既約な(部分)表現の直和，したがって V が既約な(部分)表現の直和となるからである．(*)を示そう．まず

$$V = V_1 \oplus V_1'$$

なる V の部分空間 V_1' を任意にとる．このとき，V の任意の元 v は，

$$v = v_1 + v_1' \qquad (v_1 \in V_1,\ v_1' \in V_1')$$

と一意的に書けるから，

$$\varphi(v) = v_1$$

なる V から V_1 への線型写像 φ が定義される．この φ を用いて，

$$p(v) = \frac{1}{|G|}\sum_{x \in G} \rho(x)^{-1}\varphi(\rho(x)v) \qquad (v \in V) \tag{8.8}$$

とおくと，p は V から V_1 への線型写像である．ここで k の標数が G の位数を割らないことから，$1/|G| \in k$ と考えることができることに注意．また V_1 が ρ 不変であることから $p(v) \in V_1$ がでるのである．さて p がつぎの性質を満たすことを示そう：

$$p(\rho(x)v) = \rho(x)p(v) \qquad (v \in V), \tag{8.9}$$

$$p(v) = v \qquad (v \in V_1). \tag{8.10}$$

(8.9)は，

$$\begin{aligned}
\rho(x)p(v) &= \rho(x)\left(\frac{1}{|G|}\sum_{y \in G}\rho(y)^{-1}\varphi(\rho(y)v)\right) \\
&= \frac{1}{|G|}\sum_{y \in G}\rho(x)\rho(y)^{-1}\varphi(\rho(y)v) \\
&= \frac{1}{|G|}\sum_{y \in G}\rho(yx^{-1})^{-1}\varphi(\rho(yx^{-1})\rho(x)v)
\end{aligned}$$

ここで y が G のすべての元を走るとき，yx^{-1} も G のすべての元を走ることに注意すれば，

$$\begin{aligned}
&= \frac{1}{|G|}\sum_{y \in G}\rho(y)^{-1}\varphi(\rho(y)\rho(x)v) \\
&= p(\rho(x)v)
\end{aligned}$$

となることからわかる．つぎに $v \in V_1$ とすると，$\rho(x)v \in V_1$ であるから，(8.8)

の右辺において $\varphi(\rho(x)v)=\rho(x)v$, よって

$$p(v)=\frac{1}{|G|}\sum_{x\in G}\rho(x)^{-1}\rho(x)v=\frac{1}{|G|}\sum_{x\in G}v=\frac{1}{|G|}|G|v=v$$

となり (8.10) が得られる.

p の核を V_2 としよう:

$$V_2=\{v\in V\mid p(v)=0\}.$$

このとき,

$$V=V_1\oplus V_2 \tag{8.11}$$

である. 実際,

$$\begin{aligned} V\ni v\Longrightarrow p(v-p(v)) &= p(v)-p(p(v)) \\ &= p(v)-p(v) \qquad ((8.10)\text{ による}) \\ &= 0, \end{aligned}$$

$$\therefore\quad v-p(v)\in V_2$$

となり, $v=p(v)+(v-p(v))$ より, V は V_1 と V_2 の和空間である. また $V_1\cap V_2\ni v$ とすると $v=p(v)=0$ となり, したがって (8.11) が成り立つ. つぎに V_2 が ρ 不変であることを示そう. $v\in V_2$ とすると,

$$\begin{aligned} p(\rho(x)v) &= \rho(x)p(v) \qquad ((8.9)\text{ による}) \\ &= 0, \end{aligned}$$

$$\therefore\quad \rho(x)v\in V_2$$

となり, V_2 は ρ 不変である. 以上で (*) が示され, 定理 8.1 の証明は終る. ▌

Maschke の定理から, G の位数が k の標数で割れないとき, G の k 上の表現を調べることは, 本質的には, 既約表現を調べることに帰着されることがわかる. しかし, G の位数が k の標数で割れるときには, 定理 8.1 は必ずしも成立しない. たとえば, k を標数 p の有限体として, G を

$$\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}\qquad (\alpha\in k)$$

なる形の行列全体からなる群とする. G の位数は k の元の数と等しく, それは p の巾である. ところで,

$$G\ni\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}\longmapsto\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}\in GL(2,k)$$

なる対応により，G の k 上の 2 次行列表現 ρ が得られるが，この表現 ρ は完全可約ではない．実際，$\begin{bmatrix}\beta\\0\end{bmatrix}$ $(\beta\in k)$ なる数ベクトルからなる 1 次元部分空間は ρ 不変であるが，ρ がもし完全可約であるとすると，ρ は

$$G\ni x\longmapsto\begin{bmatrix}\delta & 0\\0 & \delta'\end{bmatrix}\in GL(2,k)$$

なる行列表現と同値でなければならない．ところが，$\begin{bmatrix}\delta & 0\\0 & \delta'\end{bmatrix}$ なる形の行列からなる $GL(2,k)$ の部分群の位数は p と素であるから G の位数が p の巾であることに矛盾する．

注意 G の k 上の表現 (ρ, V) が完全可約であるとしよう．このとき，(ρ, V) は G の既約表現 (ρ_i, V_i) $(i=1,2,\cdots)$ の直和と同型であるが，これらの (ρ_i, V_i) は同型を無視して一意的に定まる．これは，V を §8.1, c) におけるように左 $k[G]$ 加群とみるとき，V_i は既約な $k[G]$ 部分加群となり，V は $V_1, V_2, \cdots$ の $k[G]$ 加群としての直和となる．とくに $V=V_1\oplus V_2\oplus\cdots$ は $k[G]$ 加群 V の直既約分解を与える．このとき (ρ_i, V_i) の同型を無視しての一意性は，Krull-Remak-Schmidt の定理 4.6 からでる ($k[G]$ 加群 V が Krull-Remak-Schmidt の定理の仮定を満たすことは読者自ら確かめよ)．なお，直既約な $k[G]$ 加群の概念に対応して，表現 (ρ, V) の直既約性も定義され，それは有限群のモジュラー表現論などにおいて大切であるが，本書ではそれには立ち入らないことにする．

§8.2 Schur の補題とその応用

本節では，有限群の表現論において基本的役割を果たす Schur の補題とその応用を示す．a) で Schur の補題を述べ，b) では代数閉体上の Abel 群の既約表現，有限群の 1 次表現の数に関する結果を述べる．c) では Schur の関係式について述べる．これは次節で説明する指標の直交関係の証明において重要である．d) では Schur の関係式の応用として標数が群の位数を割らない代数閉体上の群環の構造——定理 8.5——を述べる．

a) Schur の補題

補題 8.1 (Schur) $(\rho_1, V_1), (\rho_2, V_2)$ を有限群 G の体 k 上の既約表現，f は V_1 から V_2 への線型写像で

(8.12) $$\rho_2(x)\circ f=f\circ\rho_1(x)\qquad(\forall x\in G)$$

を満たすものとするとき，つぎの (i), (ii) が成り立つ：

(i) $f\neq 0$ ならば，f は同型写像である．したがって $f\neq 0$ のとき，(ρ_1, V_1) と (ρ_2, V_2) は同型である．

(ii) k が代数閉体で，$V_1=V_2$，$\rho_1=\rho_2$ ならば f は相似写像 (すなわち $f=\alpha 1$

($\alpha \in k$, 1 は V_1 の恒等写像)) である．

証明　(i)　$f \neq 0$ とする．f の核を V_0 とする：

$$V_0 = \{v \in V_1 \mid f(v) = 0\}.$$

この V_0 は ρ_1 不変である．実際，$v \in V_0$ のとき，$0 = \rho_2(x)f(v) = f \circ \rho_1(x)v$ より $\rho_1(x)v \in V_0$ である．さて，(ρ_1, V_1) は既約表現であるから，$V_0 = V_1$ または $\{0\}$ であるが，$V_0 = V_1$ ならば $f = 0$ となり仮定に反するから，$V_0 = \{0\}$ でなければならない．これは f が V_1 から V_2 への単射であることを示す．一方，(8.12) により $f(V_1)$ は V_2 の ρ_2 不変部分空間であり，(ρ_2, V_2) は既約であるから，$f(V_1) = V_2$ または $f(V_1) = \{0\}$ となるが，$f \neq 0$ より $f(V_1) = V_2$ でなければならない．したがって f は V_1 から V_2 の上への同型写像である[1]．

(ii)　$V_1 = V_2$，$\rho_1 = \rho_2$ としよう．f の固有値の一つを α とすると，k は代数閉体であるから，$\alpha \in k$ である．

$$g = f - \alpha 1 \qquad (1 \text{ は } V_1 \text{ の恒等変換})$$

とおくと，g は

$$\rho_1(x) \circ g = g \circ \rho_1(x) \qquad (\forall x \in G)$$

を満たす．α は f の固有値であるから，$f(v) = \alpha v$ なる $V_1 \ni v \neq 0$ が存在するから，$g(v) = 0$. よって g は同型写像ではないから，(i) により $g = 0$ すなわち $f = \alpha 1$ でなければならない．▌

以下，Schur の補題 8.1 のいくつかの大切な応用を述べよう．

b) 有限 Abel 群の既約表現

定理 8.2　G を有限 Abel 群，(ρ, V) を G の代数閉体 k 上の既約表現とすると，$\deg \rho = 1$ である．

証明　$G \ni a$ とすると，G の可換性により

$$\rho(x)\rho(a) = \rho(a)\rho(x) \qquad (\forall x \in G)$$

である．Schur の補題 8.1 の (ii) における f として $\rho(a)$ をとれば，k は代数閉体と仮定しているから，$\rho(a) = \alpha_a 1$ $(\alpha_a \in k)$ となる．したがって，(ρ, V) の既約性により $\dim V = 1$ でなければならない．▌

A を有限 Abel 群，k をその標数が A の位数を割らない代数閉体とする．

---

1)　補題 8.1 の (i) は，§7.1 で述べた補題 7.4 の特別な場合である．

Abel 群の基本定理(定理 3.4)により，A は有限巡回群 $A_1, A_2, \cdots, A_t$ の直積となる．a_i を A_i $(1 \leqq i \leqq t)$ の生成元とする：

$$A = A_1 \otimes A_2 \otimes \cdots \otimes A_t, \qquad A_i = \langle a_i \rangle \quad (1 \leqq i \leqq t).$$

a_i の位数を n_i，$\omega_i\,(\in k)$ を 1 の原始 n_i 乗根としよう (k の標数が n_i を割らないから k は 1 の原始 n_i 乗根を含む)．整数 $l_1, l_2, \cdots, l_t$ に対し

$$\text{(8.13)} \qquad \rho_{l_1 l_2 \cdots l_t}(a_i) = \omega_i^{l_i} \qquad (i=1, 2, \cdots, t)$$

によって A から k^* への準同型すなわち A の k 上の 1 次表現が定義される．明らかに

$$l_i \equiv l_i' \pmod{n_i} \quad (i=1, 2, \cdots, t) \Longrightarrow \rho_{l_1 l_2 \cdots l_t} = \rho_{l_1' l_2' \cdots l_t'},$$

$$\text{或る } i \text{ に対して } l_i \not\equiv l_i' \pmod{n_i} \Longrightarrow \rho_{l_1 l_2 \cdots l_t} \neq \rho_{l_1' \cdots l_t'}$$

であるから，(8.13)のようにして A の 1 次表現が $n_1 n_2 \cdots n_t$ 個得られる．逆に A の 1 次表現は，明らかに(8.13)のようにして得られるから，定理 8.2 と合わせてつぎの定理が得られる．

定理 8.3 A を有限 Abel 群，k をその標数が A の位数を割らない代数閉体とするとき，A の既約表現はすべて 1 次であり，A の互いに同型でない既約表現の数は，A の位数に等しい．——

G を有限群，N を G の正規部分群とする．(ρ, V) を剰余群 G/N の表現，φ を G から G/N への自然準同型とするとき，

$$\rho \circ \varphi\colon\ G \xrightarrow{\ \varphi\ } G/N \xrightarrow{\ \rho\ } GL(V)$$

は，G の表現 $(\rho \circ \varphi, V)$ を与え，$\mathrm{Ker}\,(\rho \circ \varphi) \supseteqq N$ である．逆に G の表現 (ρ, V) が $\mathrm{Ker}\,\rho \supseteqq N$ を満たすとき，ρ は G/N から $GL(V)$ への準同型すなわち (ρ, V) は G/N の表現を誘導する(問 1.27)．したがって N を核に含む G の表現と G/N の表現は 1 対 1 に対応し，この対応によって G の既約表現は G/N の既約表現に対応する．よって以後 G/N の表現を G の表現と考えたり，核が N を含む G の表現を G/N の表現と考えたりするであろう．

定理 8.4 G を有限群，k をその標数が G の位数を割らない代数閉体とする．G の k 上の 1 次表現の数は $[G : G']$ (G' は G の交換子群)に等しい．

証明 ρ を G の k 上の 1 次表現，N を ρ の核とするとき，G/N は Abel 群であるから，補題 5.2 により $N \supseteqq G'$ である．したがって上に注意したように ρ は

G/G' の1次表現とみなすことができる．逆に G/G' の1次表現は G の1次表現を与える．ところで G/G' は Abel 群であるから，定理8.3により G/G' の1次表現の数は $[G:G']$ に等しい．∎

c) Schur の関係式

$(\rho_1, V_1), (\rho_2, V_2)$ を有限群 G の k 上の既約表現，k をその標数が G の位数を割らない代数閉体とする．さて，h を V_1 から V_2 への任意の線型写像として

$$h_0 = \sum_{x \in G} \rho_2(x^{-1}) h \rho_1(x)$$

とおく．h_0 は V_1 から V_2 への線型写像であり，さらに

$$\rho_2(y) h_0 = h_0 \rho_1(y) \qquad (\forall y \in G)$$

が成り立つ．実際

$$\begin{aligned} h_0\rho_1(y) &= \sum_{x \in G} \rho_2(x^{-1}) h \rho_1(x) \rho_1(y) \\ &= \sum_{x \in G} \rho_2(x^{-1}) h \rho_1(xy) \\ &= \sum_{x \in G} \rho_2(y) \rho_2((xy)^{-1}) h \rho_1(xy) \\ &= \rho_2(y) \sum_{x \in G} \rho_2(x^{-1}) h \rho_1(x) \\ &= \rho_2(y) h_0 \end{aligned}$$

である．したがって Schur の補題8.1により

(8.14) $\qquad \rho_1 \nsim \rho_2 \Longrightarrow h_0 = 0,$

(8.15) $\qquad V_1 = V_2, \quad \rho_1 = \rho_2 \Longrightarrow h_0 = \alpha 1, \quad \alpha = \dfrac{|G| \operatorname{tr}(h)}{\deg \rho_1}$

である．ここで(8.15)の α の値は $h_0 = \alpha 1$ の両辺のトレースをとって得られるが，その際とくに $\operatorname{tr}(h) = 1$ なる V_1 から V_1 への線型写像 h をとれば $\deg \rho_1$ は k の標数で割れないことがわかることに注意せよ．

さて，V_1, V_2 のそれぞれに基底を定めて，$\rho_1(x), \rho_2(x), h$ に対応する行列を作り，それぞれ $(r_{ij}{}^1(x)), (r_{ij}{}^2(x)), (h_{ij})$ としよう．このとき，h_0 に対応する行列の (i,j) 成分 $h_{ij}{}^0$ は，

$$h_{ij}{}^0 = \sum_{x,k,l} r_{ik}{}^2(x^{-1}) h_{kl} r_{lj}{}^1(x)$$

である．(8.14)により，$\rho_1 \nsim \rho_2$ のとき $h_{ij}{}^0 = 0$ であるから μ, ν を与えたとき，(h_{ij}) として

$$h_{ij}=\begin{cases}1 & ((i,j)=(\mu,\nu)),\\ 0 & ((i,j)\neq(\mu,\nu))\end{cases}$$

なる行列をとると，

(8.16) $$\rho_1 \not\sim \rho_2 \Longrightarrow \sum_{x\in G} r_{i\mu}{}^2(x^{-1})r_{\nu j}{}^1(x)=0$$

を得る．また $V_1=V_2$，$\rho_1=\rho_2$ のとき，(8.15) より

$$\frac{|G|\ \mathrm{tr}(h)}{\deg \rho_1}\delta_{ij}=\sum_{x,k,l} r_{ik}{}^1(x^{-1})h_{kl}r_{lj}{}^1(x)$$

であるから，行列 (h_{ij}) を上のようにとって

(8.17) $$\sum_{x\in G} r_{i\mu}{}^1(x^{-1})r_{\nu j}{}^1(x)=\frac{|G|}{\deg \rho_1}\delta_{\mu\nu}\delta_{ij}$$

を得る．(8.16), (8.17) を **Schur の関係式**という．

さて，Schur の関係式の応用を示すために少し準備をしよう．G を有限群，k を任意の体とする．G から k への写像の全体を $k(G)$ によって表わす．$k(G)$ は

$$\begin{aligned}(f+g)(x)&=f(x)+g(x),\\ (\alpha f)(x)&=\alpha f(x)\end{aligned} \qquad (x\in G,\ f,g\in k(G),\ \alpha\in k)$$

なる和とスカラー積に関して，k 上の線型空間である．G の位数を n とするとき，$k(G)$ の次元は n である．実際，$G\ni x$ に対して

$$f_x(y)=\begin{cases}1 & (y=x),\\ 0 & (y\neq x)\end{cases}$$

によって $k(G)$ の元 f_x を定義すると，$\{f_x \mid x\in G\}$ が $k(G)$ の一つの基底となる．

注意 1 $k(G)\ni f,g$ に対して

(∗) $$f*g(x)=\sum_{y\in G} f(y)g(y^{-1}x)$$

によって，積 $f*g$ を定義すると，$k(G)$ は環となることがわかる．このとき，環 $k(G)$ は k 上の群環 $k[G]$ (§8.1, c)) と

(∗∗) $$k(G)\ni f\longmapsto \sum_{x\in G} f(x)x\in k[G]$$

なる対応によって同型であることが容易に確かめられる．この意味でしばしば $k(G)$ を G の k 上の群環という（あるいは群環をこのように定義する）ことがあるが，本書では混乱を避けるため $k(G)$ と $k[G]$ を記号の上で区別して扱うことにする．ただし，必要に応じて対応 (∗∗) により $k(G)$ と $k[G]$ を同一視するであろう．

注意 2 $k(G)$ を群環と定義する方が，‘形式和’という少しあいまいないい方で群環を定義するよりは，数学的には厳密である．しかし形式和を考える方が，記述が簡単になった

り，群環を感覚的に扱いやすかったりする利点もある．要するに，形式和の厳密な定義が G から k への写像であるというのが，事の真相である．

k の標数が G の位数を割らないとき，

$$(8.18) \qquad \langle f, g\rangle = \frac{1}{|G|}\sum_{x\in G} f(x)g(x^{-1})$$

とおくと，$\langle f, g\rangle$ は線型空間 $k(G)$ 上の非退化双1次形式 (nondegenerate bilinear form) である．$\langle f, g\rangle$ が双1次形式であることは明らかであろう．非退化的であることは，$\langle f, g\rangle=0$ $(\forall g\in k(G))$ とすると，$g=f_{x^{-1}}$ とおいて，$0=\langle f, f_{x^{-1}}\rangle =(1/|G|)f(x)$，よって $f(x)=0$ $(\forall x\in G)$ となることからわかる．

以下，本項 c) では k は代数閉体で，その標数は G の位数を割らないものとする．このとき，Schur の関係式 (8.16), (8.17) は，双1次形式 $\langle f, g\rangle$ を用いてつぎのように表わせる：

$(r_{ij}{}^{1}(x))$, $(r_{ij}{}^{2}(x))$ を G の k 上の既約表現 ρ_1, ρ_2 の行列表示とするとき，

$$(8.19) \qquad \rho_1 \not\sim \rho_2 \Longrightarrow \langle r_{ij}{}^{1}, r_{kl}{}^{2}\rangle = 0,$$

$$(8.20) \qquad \rho_1 = \rho_2 \Longrightarrow \langle r_{ij}{}^{1}, r_{kl}{}^{1}\rangle = \frac{1}{\deg\rho_1}\delta_{il}\delta_{jk}\text{ [1]}.$$

$\rho_1, \rho_2, \cdots, \rho_h$ を G の互いに同型でない k 上の既約表現（すべてとは限らない），その次数を $n_1, n_2, \cdots, n_h$，$(r_{ij}{}^{l}(x))$ を ρ_l の行列表示とするとき，

(8.21) $r_{ij}{}^{l}(x)$ $(1\leqq l\leqq h,\ 1\leqq i, j\leqq n_l)$ は k 上線型独立

である．実際，$\sum_{i,j,l}\alpha_{ij}{}^{l}r_{ij}{}^{l}=0$ とすると，

$$0=\left\langle \sum_{i,j,l}\alpha_{ij}{}^{l}r_{ij}{}^{l}, r_{\mu\nu}{}^{\lambda}\right\rangle = \sum_{i,j,l}\alpha_{ij}{}^{l}\langle r_{ij}{}^{l}, r_{\mu\nu}{}^{\lambda}\rangle$$
$$= \frac{1}{\deg\rho_\lambda}\sum_{i,j}\alpha_{ij}{}^{\lambda}\delta_{i\nu}\delta_{j\mu}$$
$$= \frac{1}{\deg\rho_\lambda}\alpha_{\nu\mu}{}^{\lambda},$$
$$\therefore \quad \alpha_{\nu\mu}{}^{\lambda}=0.$$

(8.21) と $k(G)$ が有限次元であることから，

(8.22) G の互いに同型でない k 上の既約表現の数は有限

であることがわかる．つぎの項 d) において，群環 $k[G]$ の構造を調べて，互い

---

1) 先を急ぐ読者は，ここから直ちに§8.3に進んでもよい．

に同型でない既約表現の数は G の共役類の数に等しいことを見るであろう．さて，h を G の互いに同型でない既約表現の数とするとき，

(8.23) (8.21) における $r_{ij}{}^{l}$ $(1\leqq l\leqq h,\ 1\leqq i,j\leqq n_l)$ は $k(G)$ の底である．とくに $|G|=n_1{}^2+n_2{}^2+\cdots+n_h{}^2$

であることを示そう．U を $r_{ij}{}^{l}$ $(1\leqq l\leqq h,\ 1\leqq i,j\leqq n_l)$ で生成される $k(G)$ の部分空間，$U^{\perp}=\{f\in k(G)\mid \langle f,r_{ij}{}^{l}\rangle=0\ (1\leqq l\leqq h,\ 1\leqq i,j\leqq n_l)\}$ とおく．$\langle f,g\rangle$ の非退化性により，$\dim U^{\perp}=|G|-\dim U$ (実際は，$\langle f,g\rangle$ が U の上で非退化であるから，$k(G)=U\oplus U^{\perp}$) であるから，(8.23) を示すには，$U^{\perp}=\{0\}$ をいえばよい．$U^{\perp}\ni f$ と G の k 上の任意の表現 (ρ,V) に対して

$$\rho(f)=\sum_{x\in G}f(x)\rho(x^{-1})$$

とおく．$\rho(f)$ は V の線型変換である．また

(8.24) $$\rho=\rho_1\oplus\cdots\oplus\rho_m \Longrightarrow \rho(f)=\rho_1(f)\oplus\cdots\oplus\rho_m(f)$$

である．(ρ,V) が既約ならば，$\rho(f)$ の行列表示を考えると，$U^{\perp}$ の定義により $\rho(f)=0$ であるから，Maschke の定理 8.1 と (8.24) から，任意の表現 (ρ,V) に対して $\rho(f)=0$ を得る．そこで，(ρ,V) として G の正則表現 $(1^G,k[G])$ をとる (例 8.6)：

$$1^G(x)\Bigl(\sum_{y\in G}a_y y\Bigr)=\sum_{y\in G}a_y xy.$$

このとき，

$$0=1^G(f)(1)=\sum_{x\in G}f(x)1^G(x^{-1})1=\sum_{x\in G}f(x)x^{-1},$$

$$\therefore\quad f(x)=0 \qquad (\forall x\in G).$$

したがって $U^{\perp}=\{0\}$ となり，(8.23) が示された．

d) 群環の構造

群環 $k[G]$ (k はその標数が G の位数を割らない代数閉体) の構造を調べるために，最初に多元環について簡単に説明しよう．

k を任意の体とする．k 上の線型空間 A が環の構造をもち，

$$\alpha(xy)=(\alpha x)y=x(\alpha y) \qquad (\alpha\in k,\ x,y\in A)$$

が成り立つとき，A を k 上の**多元環**あるいは**線型環**という．本書では，単位元をもつ環だけを考えているから，

$$\alpha x = \alpha(1x) = (\alpha 1)x = x(\alpha 1) \qquad (\alpha \in k,\ 1 \text{ は } A \text{ の単位元})$$

となり，A の右イデアル，左イデアル，両側イデアルは必然的に線型空間 A の部分空間となる．

例 8.7 （i） 体 k 上の行列環 $M_n(k)$ は k 上の多元環である．

（ii） Hamilton の4元数体 $\boldsymbol{H}$ (p. 40 参照) は実数体 $\boldsymbol{R}$ 上の多元環である．

(iii) G を有限群，k を体とするとき，G の k 上の群環 $k[G]$ は k 上の多元環である．——

$A_1, A_2, \cdots, A_h$ を体 k 上の多元環とするとき，直積集合 $A_1 \times A_2 \times \cdots \times A_h$ は

$$(a_1, a_2, \cdots, a_h) + (b_1, b_2, \cdots, b_h) = (a_1+b_1, \cdots, a_h+b_h),$$
$$(a_1, \cdots, a_h)\cdot(b_1, \cdots, b_h) = (a_1b_1, \cdots, a_hb_h), \qquad (a_i, b_i \in A_i,\ \alpha \in k)$$
$$\alpha(a_1, a_2, \cdots, a_h) = (\alpha a_1, \cdots, \alpha a_h)$$

なる演算に関して k 上の多元環となる．これを

$$A_1 \oplus A_2 \oplus \cdots \oplus A_h$$

と書き，$A_1, A_2, \cdots, A_h$ の**直和**という．$A = A_1 \oplus \cdots \oplus A_h$ のとき，A_i の元 a_i と A の元 $(0, \cdots, \overset{i}{\breve{a_i}}, \cdots, 0)$ を同一視して A_i を A の部分集合と考えるとき，A_i は A の両側イデアルであり，さらに

(α) 線型空間 A は，部分空間 A_i $(1 \leqq i \leqq h)$ の直和，

(β) $a_ia_j = 0 \quad (i \neq j,\ a_i \in A_i,\ a_j \in A_j)$

である．逆に k 上の多元環 A の両側イデアル $A_1, A_2, \cdots, A_h$ が (α), (β) を満たすとしよう．このとき，(α) により A の各元 a は

$$a = a_1 + a_2 + \cdots + a_h \qquad (a_i \in A_i)$$

の形に一意的に書き表わされる．また A の単位元 1 を

$$1 = e_1 + \cdots + e_h \qquad (e_i \in A_i)$$

と書くと，各 A_i は e_i を単位元としてもつ k 上の多元環である．ただし，A と A_i は単位元を共有しないから，本書の意味では，A_i は A の部分環ではない(p. 39 参照)．さて，写像

$$A \ni a = a_1 + \cdots + a_h \longmapsto (a_1, \cdots, a_h) \in A_1 \oplus \cdots \oplus A_h$$

により，多元環としての同型

$$A \simeq A_1 \oplus \cdots \oplus A_h$$

が得られるから，A の両側イデアル $A_1, A_2, \cdots, A_h$ が $(\alpha), (\beta)$ を満たすとき，簡単に

$$A = A_1 \oplus \cdots \oplus A_h$$

と書くことにしよう．

多元環 A に対して

$$Z(A) = \{z \in A \mid xz = zx \ (\forall x \in A)\}$$

とおくと，$Z(A)$ は A の可換な部分環でしかも A の部分空間である．$Z(A)$ を A の**中心**という．群環 $k[G]$ の中心は，h 次元部分空間(h は G の共役類の数)であった(§8.1, c))．

$$A = A_1 \oplus \cdots \oplus A_h$$

のとき，

$$Z(A) = Z(A_1) \oplus \cdots \oplus Z(A_h)$$

であることは容易にわかる．

問 8.5 これを確かめよ．

問 8.6 k 上の行列環 $M_n(k)$ の中心は，スカラー行列全体からなることを示せ．また Hamilton の 4 元数体の中心を求めよ．

問 8.7 $k(G) \ni f, g$ に対して $(fg)(x) = f(x)g(x)$ $(x \in G)$ によって積を定義するとき，

$$k(G) \simeq \underbrace{k \oplus \cdots \oplus k}_{n} \qquad (n = |G|)$$

を示せ．

定理 8.5 G を有限群，k をその標数が G の位数を割らない代数閉体とする．$n_1, n_2, \cdots, n_h$ を G のすべての互いに同型でない k 上の既約表現の次数とするとき，

$$k[G] \simeq M_{n_1}(k) \oplus \cdots \oplus M_{n_h}(k).$$

証明 §8.2, c) の注意 1 における対応 (**) によって $k(G)$ と $k[G]$ を同一視する．このとき，$k(G)$ における積は，そこの (*) で与えられることに注意．G の h 個の既約表現のそれぞれに対して，一つの行列表示

$$(r_{ij}{}^{l}(x)) \qquad (1 \leqq l \leqq h, \ 1 \leqq i, j \leqq n_l)$$

をとり，A_l を $r_{ij}{}^{l}(x)$ $(1 \leqq i, j \leqq n_l)$ の線型結合の全体とする．まず，A_l は $k(G)$

の両側イデアルである．実際，$k(G) \ni f$ とすると，

$$\begin{aligned} f * r_{ij}{}^{l}(x) &= \sum_{y\in G} f(y) r_{ij}{}^{l}(y^{-1}x) \\ &= \sum_{y\in G} f(y) \sum_{t} r_{it}{}^{l}(y^{-1}) r_{tj}{}^{l}(x) \\ &= \sum_{t} \left(\sum_{y\in G} f(y) r_{it}{}^{l}(y^{-1}) \right) r_{tj}{}^{l}(x) \in A_l, \\ r_{ij}{}^{l} * f(x) &= \sum_{y\in G} r_{ij}{}^{l}(y) f(y^{-1}x) \in A_l. \end{aligned}$$

つぎに，

(i) $A_l \simeq M_{n_l}(k)$,

(ii) $s \neq t$, $A_s \ni a_s$, $A_t \ni a_t \Longrightarrow a_s * a_t = 0$

を示そう．

$$\begin{aligned} r_{ij}{}^{s} * r_{kl}{}^{t}(x) &= \sum_{y\in G} r_{ij}{}^{s}(y) r_{kl}{}^{t}(y^{-1}x) \\ &= \sum_{y\in G} r_{ij}{}^{s}(y) \left(\sum_{u} r_{ku}{}^{t}(y^{-1}) r_{ul}{}^{t}(x) \right) \\ &= \sum_{u} \left(\sum_{y\in G} r_{ij}{}^{s}(y) r_{ku}{}^{t}(y^{-1}) \right) r_{ul}{}^{t}(x) \\ &= \sum_{u} |G| \langle r_{ij}{}^{s}, r_{ku}{}^{t} \rangle r_{ul}{}^{t}(x) \\ &= \sum_{u} \frac{|G|}{n_t} \delta_{iu}\delta_{jk}\delta_{st} r_{ul}{}^{t}(x) \qquad \text{(Schur の関係式)}. \end{aligned}$$

よって

$$s \neq t \Longrightarrow r_{ij}{}^{s} * r_{kl}{}^{t} = 0,$$
$$s = t \Longrightarrow r_{ij}{}^{s} * r_{kl}{}^{s} = \frac{|G|}{n_s} \delta_{jk} r_{il}{}^{s}$$

を得る．したがって

$$e_{ij}{}^{l} = \frac{n_s}{|G|} r_{ij}{}^{l}$$

とおくと，

(8.25) $$e_{ij}{}^{s} * e_{kl}{}^{t} = \delta_{st}\delta_{jk} e_{il}{}^{s}$$

となる．A_l の元は $e_{ij}{}^{l}$ $(1 \leqq i, j \leqq n_l)$ の線型結合であるから，(8.25) から上の (ii) がでる．また，$E_{ij}{}^{l}$ によって (i, j) 成分のみ 1 で他の成分はすべて 0 である n_l 次

行列を表わせば，(8.25) は

$$e_{ij}^{\ l} \longmapsto E_{ij}^{\ l}$$

なる対応によって

$$A_l \simeq M_{n_l}(k)$$

であることを示す．すなわち (i) が示された．ところで (8.23) により $k(G)$ は $A_1, A_2, \cdots, A_h$ の (線型空間としての) 直和であるから，(i), (ii) と合わせて多元環としての同型

$$k(G) \simeq M_{n_1}(k) \oplus \cdots \oplus M_{n_h}(k)$$

が得られる．▌

系 G, k を定理 8.5 の通りとする．G の互いに同型でない k 上の既約表現の数は，G の共役類の数に等しい．

証明 $k(G)$ の中心の次元は，G の共役類の数に等しい．一方，$M_{n_1}(k) \oplus \cdots \oplus M_{n_h}(k)$ の中心の次元は，$M_n(k)$ の中心の次元が 1 であるから (問 8.6)，h である．ところが，h は互いに同型でない既約表現の数であった．▌

Schur の関係式の応用として，(8.23)，定理 8.5 の系において，有限群の既約表現についての重要な結果が導かれた．これらの結果は，つぎの節で複素数体上の表現に対して，指標の理論の応用としてもう一度証明するであろう．

一般の (とくに代数的に閉じていない) 体 k 上の群環の構造についても，いろいろなことが知られている．これらの事実に基づいて，有限群の表現論を本書とは異なったもっと環論的に取り扱う方法もある．これらは，理論的にも応用上も (とくにモジュラー表現論などより進んだ表現論に対しては) 非常に大切なのであるが，本書ではそれには全然立ち入らない．この有限群の表現論の環論的扱いに興味のある読者は，

秋月康夫，鈴木通夫：代数 II (岩波全書)，

服部昭：群とその表現 (共立出版)

を参照されたい．

問 8.8 位数 8 の正 2 面体群 D_8 と位数 8 の 4 元数群 Q_8 の**実数体** $\boldsymbol{R}$ 上の群環はつぎのようになることを示せ：

$$\boldsymbol{R}[D_8] \simeq \boldsymbol{R} \oplus \boldsymbol{R} \oplus \boldsymbol{R} \oplus \boldsymbol{R} \oplus M_2(\boldsymbol{R}),$$

$$\boldsymbol{R}[Q_8] \simeq \boldsymbol{R} \oplus \boldsymbol{R} \oplus \boldsymbol{R} \oplus \boldsymbol{R} \oplus \boldsymbol{H} \qquad (\boldsymbol{H} \text{ は Hamilton の 4 元数体}).$$

［ヒント］　例8.3-8.4で与えた D_8, Q_8 の表現を利用せよ．

§8.3　指標とその直交関係

この節では，有限群の複素数体上の表現に対して指標を定義し，その基本性質——直交関係など——を説明する．指標の重要性は，表現の同型が指標の一致と同値である点にある．また指標のいろいろな性質は，表現論や有限群論に有効な応用をもつ．とくに指標の値は，1の巾根の和であるから，そのような数の整数論的性質から，しばしば群指標について興味深い結果が得られる．そのような例として，c)では“既約表現の次数は群の位数を割る”という基本的な結果を証明し，d)ではBurnsideによるいくつかの結果を述べる．とくに第7章で証明を省略したいわゆるBurnsideの $p^a\cdot q^b$ 定理(p. 165)の証明を与える．

本節以降，本書では複素数体上の表現のみを考える．したがって‘$\boldsymbol{C}$ 上の’という言葉を省略することもあるであろう．

a)　指　標

(ρ, V) を有限群 G の複素数体 $\boldsymbol{C}$ 上の表現とする．$G\ni x$ に対して

$$\chi_\rho(x) = \mathrm{tr}\,(\rho(x))$$

とおく．右辺は V の線型変換 $\rho(x)$ のトレースである．すなわち (ρ, V) の行列表示 $R(x)$ をとり，$R(x)$ の対角成分の和が $\mathrm{tr}\,(\rho(x))$ である：

$$\mathrm{tr}(\rho(x)) = \sum_{i=1}^{n} r_{ii}(x) \qquad (R(x)=(r_{ij}(x)),\ \ n=\deg\rho).$$

$\mathrm{tr}\,(S^{-1}\rho(x)S)=\mathrm{tr}\,(\rho(x))$ (S は正則行列)であるから，$\chi_\rho(x)$ は (ρ, V) の行列表示のとり方によらず定まる G 上定義された複素数値関数である．χ_ρ を表現 (ρ, V) の**指標**(character)という．ρ が G の既約表現であるとき，χ_ρ を**既約指標**という．恒等表現の指標は**恒等指標**あるいは**自明な(既約)指標**といわれる．また指標の**次数**，**核**，**忠実**などは，対応する表現の次数，核，忠実のことである．

補題8.2　(i)　$\rho_1\sim\rho_2 \Longrightarrow \chi_{\rho_1}=\chi_{\rho_2}$.

(ii)　$\chi_\rho(y^{-1}xy)=\chi_\rho(x)$ $(\forall x, y\in G)$．すなわち指標は G の各共役類の上で一定の値をとる．

(iii)　$\chi_\rho(x^{-1}) = \overline{\chi_\rho(x)}$　（$\overline{\ }$ は複素共役を表わす）．

(iv)　$\chi_\rho(x) = \chi_\rho(1) \Longleftrightarrow \rho(x) = 1_V$　(1_V は V の恒等変換)，
　　すなわち　$\mathrm{Ker}\,\rho = \{x\in G \mid \chi_\rho(x)=\chi_\rho(1)\}$.

(v)　ρ が既約のとき，$\chi_\rho(zx)=\chi_\rho(z)\chi_\rho(x)/\chi_\rho(1)$ $(x\in G,\ \ z\in Z(G))$.

証明 一般に $\mathrm{tr}(B^{-1}AB)=\mathrm{tr}(A)$ (A, B は同次数の正方行列) である．$\rho_1\sim\rho_2$ すなわち

$$S^{-1}\rho_1(x)S=\rho_2(x) \qquad (\forall x\in G)$$

が成り立てば，

$$\chi_{\rho_1}(x)=\mathrm{tr}(S^{-1}\rho_1(x)S)=\mathrm{tr}(\rho_2(x))=\chi_{\rho_2}(x).$$

すなわち，(i) が成り立つ．$A=\rho(x)$，$B=\rho(y)$ とおけば，(ii) を得る．$G\ni x$ の位数を m としよう．このとき $\rho(x)^m=1$ であるから $\rho(x)$ は対角化可能($\rho(x)$ の最小多項式は X^m-1 の約数で重根をもたないことに注意)となり，

$$S_x^{-1}\rho(x)S_x=\begin{bmatrix}\omega_1 & & & 0\\ & \omega_2 & & \\ & & \ddots & \\ 0 & & & \omega_n\end{bmatrix}$$

なる正則行列 S_x が存在する．このとき，$\omega_i^m=1$ $(1\leqq i\leqq n)$ すなわち $\rho(x)$ の固有値 ω_i は 1 の m 乗根である．よって

$$\overline{\omega}_i=\omega_i^{-1} \qquad (i=1,2,\cdots,n)$$

となる．ところで，

$$S_x^{-1}\rho(x^{-1})S_x=\begin{bmatrix}\omega_1^{-1} & & & \\ & \omega_2^{-1} & & \\ & & \ddots & \\ & & & \omega_n^{-1}\end{bmatrix}$$

であるから，

$$\begin{aligned}\chi_\rho(x^{-1})&=\omega_1^{-1}+\cdots+\omega_n^{-1}\\&=\overline{\omega}_1+\cdots+\overline{\omega}_n\\&=\overline{\omega_1+\omega_2+\cdots+\omega_n}\\&=\overline{\chi_\rho(x)}.\end{aligned}$$

すなわち (iii) を得る．

$$n=\chi_\rho(1)=\chi_\rho(x)=\omega_1+\omega_2+\cdots+\omega_n$$

としよう．

$$|\omega_1+\omega_2+\cdots+\omega_n|\leqq|\omega_1|+|\omega_2|+\cdots+|\omega_n|=\underbrace{1+1+\cdots+1}_{n}=n$$

で，等号は $\omega_1=\omega_2=\cdots=\omega_n$ のときに限り成り立つから，

$$\chi_\rho(1)=\chi_\rho(x) \Leftrightarrow \omega_1=\omega_2=\cdots=\omega_n=1$$
$$\Leftrightarrow \rho(x)=1_V.$$

すなわち(iv)を得る．ρ を既約表現としよう．$z\in Z(G)$ のとき，Schur の補題8.1の(ii)により，$\rho(z)$ はスカラー変換である：

$$\rho(z)=\alpha 1_V,$$
$$\therefore\quad \chi_\rho(z)=\alpha\chi_\rho(1).$$

このとき $\rho(zx)=\alpha\rho(x)$ $(\forall x\in G)$ であるから，両辺のトレースをとって，$\chi_\rho(zx)=\alpha\chi_\rho(x)=\chi_\rho(z)\chi_\rho(x)/\chi_\rho(1)$ を得る．▌

補題8.2の(i)により同型な表現の指標は一致する．後にこの逆が成立すること，すなわち指標が一致する二つの表現は同型であることを見るであろう(定理8.7)．また補題8.2の(iv)は，指標を用いて自明でない正規部分群を見出す原理を示している．すなわち，自明でない指標 χ に対して，$\chi(x)=\chi(1)$ なる $G\ni x\neq 1$ が存在すれば，χ の核は G の自明でない正規部分群である．指標の理論の有限群論への応用は，すべてこの簡単な事実に基づくのである．

ρ_1,ρ_2 を G の表現とするとき，

(8.26) $$\rho=\rho_1\oplus\rho_2 \Longrightarrow \chi_\rho=\chi_{\rho_1}+\chi_{\rho_2},$$

(8.27) $$\rho=\rho_1\otimes\rho_2 \Longrightarrow \chi_\rho=\chi_{\rho_1}\chi_{\rho_2}$$

であることが，表現の和，テンソル積の定義からわかる．

例 8.8 置換表現の指標 G が有限集合 Ω に作用しているとき，これから G の置換表現が得られる(例8.2)．その指標を χ とすると，$\chi(x)$ $(x\in G)$ は，x の Ω における固定点の数に等しいことが，置換表現の定義から容易にわかる：

(8.28) $$\chi(x)=|\{v\in\Omega\mid x\circ v=v\}|.$$

また，$\Omega_1,\Omega_2,\cdots,\Omega_t$ を (G,Ω) の軌道の全体とするとき，(G,Ω) から得られる置換表現 ρ は，(G,Ω_i) $(i=1,2,\cdots,t)$ から得られる置換表現 ρ_i の和であるから(例8.5)，(8.26)により，

(8.29) $$\chi_\rho=\chi_{\rho_1}+\cdots+\chi_{\rho_t}$$

を得る．H を G の任意の部分群，

$$G=x_1H+\cdots+x_nH \qquad (n=[G:H])$$

を G の H による左剰余類分解とするとき，置換表現 $1_H{}^G$ の指標を同じ記号 $1_H{}^G$ で表わせば，(8.28)により

$$1_H{}^G(x) = (xx_iH = x_iH \text{ なる } i \text{ の数})$$

である．とくに $H=\{1\}$ とすれば，正則表現 1^G の指標は，

$$1^G(x) = \begin{cases} |G| & (x=1), \\ 0 & (x \neq 1) \end{cases} \tag{8.30}$$

となる．K を G の部分群として，K の G/H への作用から得られる K の置換表現を考えよう．

$$G = Kx_1H + Kx_2H + \cdots + Kx_tH$$

を G の K, H による両側分解とするとき，各 i に対して両側剰余類 Kx_iH に含まれる H の左剰余類の全体は $(K, G/H)$ の軌道であり，x_iH の固定部分群は $x_iHx_i{}^{-1} \cap K$ であるから，この軌道への K の作用は $(K, K/\tilde{K}_i)$ $(\tilde{K}_i = x_iHx_i{}^{-1} \cap K)$ と同型である．これから，$x \in K$ に対して

$$1_H{}^G(x) = \sum_{i=1}^{t} 1_{\tilde{K}_i}{}^K(x) \qquad (x \in K)$$

となる．すなわち，指標 $1_H{}^G$ の K への制限を $1_H{}^G \,|\, K$ で表わせば，

$$1_H{}^G \,|\, K = \sum_{i=1}^{t} 1_{\tilde{K}_i}{}^K \qquad (\tilde{K}_i = x_iHx_i{}^{-1} \cap K) \tag{8.31}$$

である．(8.31) は，後に説明される **Mackey 分解**(§8.4, e) 定理 8.23) とよばれるものの特別な場合であり，後にときどき用いられる．

b) 指標の直交関係

$\boldsymbol{C}(G)$ を，§8.2, c) におけるように G 上で定義された複素数値関数全体の作る線型空間とする．$\boldsymbol{C}(G)$ 上には

$$\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) g(x^{-1})$$

なる非退化双1次形式が定義されていた．ここで，$\langle f, g \rangle$ と異なる半双1次形式を定義しよう：

$$(f, g) = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$$

とおくと，(f, g) は線型空間 $\boldsymbol{C}(G)$ 上の正値 Hermite 形式である．(f, g) を**内積**ということがある．χ_1, χ_2 が G の指標ならば，補題 8.2 の (iii) により $\chi_i(x^{-1}) = \overline{\chi_i(x)}$ $(x \in G)$ であるから，

$$(\chi_1, \chi_2) = \langle \chi_1, \chi_2 \rangle$$

である.

定理 8.6(既約指標の第1直交関係) χ_1, χ_2 をそれぞれ G の既約表現 ρ_1, ρ_2 の指標とするとき,

(i) $\rho_1 \nsim \rho_2 \Longrightarrow (\chi_1, \chi_2) = 0$,

(ii) $\rho_1 \sim \rho_2 \Longrightarrow \chi_1 = \chi_2$, $(\chi_1, \chi_1) = 1$.

証明 ρ_1, ρ_2 の行列表示をそれぞれ $(r_{ij}{}^1(x)), (r_{kl}{}^2(x))$ とするとき,

$$\chi_1(x) = \sum_{i=1}^{m} r_{ii}{}^1(x) \qquad (m = \deg \rho_1),$$

$$\chi_2(x) = \sum_{j=1}^{n} r_{jj}{}^2(x) \qquad (n = \deg \rho_2)$$

である. また, Schur の関係式 (8.19), (8.20) により

$$\text{(8.32)} \qquad \begin{aligned} &\rho_1 \nsim \rho_2 \Longrightarrow \langle r_{ij}{}^1(x), r_{kl}{}^2(x)\rangle = 0, \\ &\rho_1 \sim \rho_2 \Longrightarrow \langle r_{ij}{}^1(x), r_{kl}{}^1(x)\rangle = \frac{1}{m}\delta_{il}\delta_{jk} \end{aligned}$$

である. まず $\rho_1 \nsim \rho_2$ としよう. そのとき,

$$\begin{aligned} (\chi_1, \chi_2) &= \left\langle \sum_{i=1}^{m} r_{ii}{}^1(x), \sum_{j=1}^{n} r_{jj}{}^2(x) \right\rangle \\ &= \sum_{i,j} \langle r_{ii}{}^1(x), r_{jj}{}^2(x)\rangle \\ &= 0 \qquad \text{((8.32) の最初の式による)}. \end{aligned}$$

つぎに $\rho_1 \sim \rho_2$ とすると, まず補題 8.2 の (i) により $\chi_1 = \chi_2$.

$$\begin{aligned} (\chi_1, \chi_1) &= \left\langle \sum_{i=1}^{m} r_{ii}{}^1(x), \sum_{j=1}^{m} r_{jj}{}^1(x) \right\rangle \\ &= \sum_{i,j} \langle r_{ii}{}^1(x), r_{jj}{}^1(x)\rangle \\ &= \sum_{i,j} \frac{1}{m}\delta_{ij} \qquad \text{((8.32) の第2式による)} \\ &= \frac{1}{m}\cdot m = 1. \end{aligned}$$

∎

第1直交関係からの直接の帰結として, まず

(8.33) 有限群の二つの既約表現が同型であるためにはそれらの指標が一致することが必要十分である

ことがわかる. さらに,

(8.34) 互いに同型でない既約表現の数は有限である[1]．

実際，$\rho_1, \rho_2, \cdots$ を互いに同型でない既約表現の全体，それらの指標をそれぞれ $\chi_1, \chi_2, \cdots$ とすると，定理 8.6 により $\chi_1, \chi_2, \cdots$ は $\boldsymbol{C}(G)$ の内積 (f, g) に関して直交するから，それらは $\boldsymbol{C}$ 上線型独立である．$\boldsymbol{C}(G)$ は有限次元であるから，$\chi_1, \chi_2, \cdots$ も有限個でなければならない．このとき，(8.34) は (8.33) からでる．(8.33), (8.34) は後に精密化される (定理 8.7，定理 8.9)．

$\rho_1, \rho_2, \cdots, \rho_h$ を G の互いに同型でない既約表現の全体，$\chi_1, \chi_2, \cdots, \chi_h$ をそれぞれの指標とする．ρ を G の任意の表現とするとき，Maschke の定理 8.1 により ρ はいくつかの既約表現の和に分解されるが，ρ_i と同型なものが m_i 個現われたものとしよう．このとき，ρ は

$$\underbrace{\rho_1\oplus\cdots\oplus\rho_1}_{m_1}\oplus\underbrace{\rho_2\oplus\cdots\oplus\rho_2}_{m_2}\oplus\cdots\oplus\underbrace{\rho_h\oplus\cdots\oplus\rho_h}_{m_h}$$

と同型である．以後，このことを簡単に

$$\rho \sim m_1\rho_1\oplus m_2\rho_2\oplus\cdots\oplus m_h\rho_h$$

と表わし，これを ρ の既約表現への**分解**，また m_i を ρ における ρ_i の**重複度**という．このとき，ρ の指標 χ は

$$(*) \qquad \chi = m_1\chi_1 + m_2\chi_2 + \cdots + m_h\chi_h$$

と書き表わされ，既約指標の第 1 直交関係により，

$$m_i = (\chi, \chi_i) \qquad (i=1, 2, \cdots, h)$$

である．$(*)$ を χ の既約指標への**分解**という．また，$m_i \neq 0$ のとき，ρ_i または χ_i をそれぞれ ρ または χ の**既約成分**ということがある．

定理 8.7 有限群 G の二つの表現が同型であるためには，それらの指標が一致することが必要十分である．

証明 ρ, ρ' を G の表現，それらの指標がともに χ であったとしよう．

$$\rho \sim m_1\rho_1\oplus\cdots\oplus m_h\rho_h,$$
$$\rho' \sim m_1'\rho_1\oplus\cdots\oplus m_h'\rho_h$$

を ρ, ρ' の既約表現への分解とすれば，上に述べたことから，

$$m_i = (\chi, \chi_i) = m_i'$$

1) (8.34) およびつぎの定理 8.9 は，すでに §8.2, c), d) において別の方法で証明されている．

となり，これは $\rho\sim\rho'$ を示す．▌

定理 8.8　χ を表現 ρ の指標とする．ρ が既約表現であるためには，$(\chi,\chi)=1$ であることが必要十分である．

証明　必要であることは，定理 8.6 の (ii) にほかならない．逆に $\rho\sim m_1\rho_1\oplus\cdots\oplus m_h\rho_h\ (m_i\geqq 0)$ を ρ の既約表現への分解とするとき，$\chi=m_1\chi_1+\cdots+m_h\chi_h$ であり $(\chi,\chi)=1$ ならば，

$$1=(\chi,\chi)=\left(\sum_{i=1}^h m_i\chi_i,\ \sum_{i=1}^h m_i\chi_i\right)$$

$$=\sum_{i,j} m_i m_j\delta_{ij}=\sum_{i=1}^h m_i{}^2$$

より，或る i に対して $m_i=1$，$j\neq i$ のとき $m_j=0$ すなわち $\rho\sim\rho_i$ となり，ρ は既約表現である．▌

例 8.9　正則表現の既約表現への分解　χ を G の既約指標，1^G を G の正則表現の指標とするとき，(8.30) により

$$(1^G,\chi)=\frac{1}{|G|}\sum_{x\in G}1^G(x)\overline{\chi(x)}=\frac{1}{|G|}|G|\chi(1)=\chi(1)$$

であるから，正則表現の既約表現への分解は各既約表現をその次数だけ含むことがわかる．とくに $\chi_1,\cdots,\chi_h$ を G の既約指標の全体とするとき

$$1^G=\chi_1(1)\chi_1+\chi_2(1)\chi_2+\cdots+\chi_h(1)\chi_h$$

が正則表現の指標の既約指標への分解である．とくに両辺の単位元における値を比べて

$$|G|=\chi_1(1)^2+\chi_2(1)^2+\cdots+\chi_h(1)^2$$

を得る．この式は §8.2, c) (8.23) において別の方法で証明されたものである．

——

$C(G)\ni f$ は，

$$f(x)=f(y^{-1}xy)\qquad(\forall x,y\in G)$$

を満たすとき，**類関数** (class function) といわれる．類関数は G の各共役類の上で一定の値をとる関数である．補題 8.2 の (ii) により，G の指標は類関数である．$Cl(G)$ によって G の類関数全体の集合を表わそう．$Cl(G)$ は $C(G)$ の部分空間で，その次元は G の共役類の数に等しい．実際，$K_1,K_2,\cdots,K_l$ を G の共役類の全体とするとき，

$$f_i(x) = \begin{cases} 1 & (x \in K_i), \\ 0 & (x \notin K_i) \end{cases}$$

とおくと，$f_1, f_2, \cdots, f_l$ が $Cl(G)$ の一つの基底となるからである．

問 8.9　§8.2, c) における注意1で述べた $\boldsymbol{C}(G)$ と群環 $\boldsymbol{C}[G]$ の同型対応 $(**)$ によって，$Cl(G)$ は $\boldsymbol{C}[G]$ の中心に対応することを確かめよ．

定理 8.9　G の既約指標の全体 $\chi_1, \chi_2, \cdots, \chi_h$ は $Cl(G)$ の正規直交基底である．とくに G の互いに同型でない既約表現の数は，G の共役類の数に等しい．

証明[1]　G の任意の表現 (ρ, V) と $f \in Cl(G)$ に対して

$$(*) \qquad \rho(f) = \sum_{x \in G} f(x) \rho(x^{-1})$$

とおく．$\rho(f)$ は V の線型変換である．$\rho = \rho_1 \oplus \rho_2 \oplus \cdots \oplus \rho_t$ のとき，

$$(**) \qquad \rho(f) = \rho_1(f) \oplus \cdots \oplus \rho_t(f)$$

である．また簡単な計算により

$$\rho(f)\rho(y) = \rho(y)\rho(f) \qquad (\forall y \in G)$$

が成り立つことがわかる．したがって ρ が G の既約表現ならば，Schur の補題 8.1 により，$\rho(f)$ はスカラー変換であるが，$(*)$ の両辺のトレースをとって

$$(***) \qquad \rho(f) = \alpha 1_V, \qquad \alpha = \frac{|G|}{\chi(1)}(f, \chi) \quad (\chi \text{ は } \rho \text{ の指標})$$

であることがわかる．さて $\chi_1, \chi_2, \cdots, \chi_h$ によって張られる $Cl(G)$ の部分空間を U，U の直交補空間を $U^\perp$ とする：

$$U^\perp = \{f \in Cl(G) \mid (f, \chi_i) = 0 \ (1 \leqq i \leqq h)\}.$$

$Cl(G) = U \oplus U^\perp$ であるから，定理 8.9 を示すには $U^\perp = \{0\}$ をいえばよい．$U^\perp \ni f$ とすると，既約表現 ρ に対しては $(***)$ により $\rho(f) = 0$ であるから，$(**)$ により G の任意の表現 (ρ, V) に対して，$\rho(f) = 0$ であることがわかる．そこで G の正則表現 $(1^G, \boldsymbol{C}(G))$ を考えよう（例 8.6）．このとき

$$1^G(x)\left(\sum_{y \in G} a_y y\right) = \sum_{y \in G} a_y xy$$

であるから，

$$0 = 1^G(f)(1) = \sum_{x \in G} f(x) 1^G(x^{-1}) 1 = \sum_{x \in G} f(x) x^{-1} \qquad (f \in U^\perp),$$

---

1)　§8.2, c) における (8.23) の証明と同じやり方である．

$$\therefore \quad f(x)=0 \qquad (\forall x \in G).$$

すなわち $f=0$ である．▌

定理 8.10（既約指標の第2直交関係） $\chi_1, \chi_2, \cdots, \chi_h$ を G の既約指標全体とするとき，

$$\sum_{i=1}^{h} \chi_i(x)\overline{\chi_i(y)} = \begin{cases} 0 & (x \text{ と } y \text{ が } G \text{ で共役でないとき}), \\ |C_G(x)| & (x \text{ と } y \text{ が } G \text{ で共役のとき}) \end{cases}$$

が成り立つ．ここで $C_G(x)$ は x の G における中心化群を表わす．

証明 $G \ni x$ に対して

$$f_x(y) = \begin{cases} 1 & (y \text{ が } x \text{ と共役のとき}), \\ 0 & (y \text{ が } x \text{ と共役でないとき}) \end{cases}$$

とおくと，$f_x \in Cl(G)$ である．定理 8.9 により

$$f_x = \sum_{i=1}^{h} \lambda_i \chi_i \qquad (\lambda_i \in \boldsymbol{C})$$

であるが，第1直交関係（定理 8.6）を用いて

$$(f_x, \chi_i) = \left(\sum_{j=1}^{h} \lambda_j \chi_j, \chi_i\right) = \lambda_i.$$

一方，x と共役な y の個数は $|G|/|C_G(x)|$ であるから，

$$\begin{aligned} (f_x, \chi_i) &= \frac{1}{|G|}\sum_{y \in G} f_x(y)\overline{\chi_i(y)} \\ &= \frac{1}{|G|}\frac{|G|}{|C_G(x)|}\overline{\chi_i(x)} \\ &= \frac{1}{|C_G(x)|}\overline{\chi_i(x)}. \end{aligned}$$

よって，

$$|C_G(x)| f_x = \sum_{i=1}^{h} \overline{\chi_i(x)} \chi_i$$

を得る．これは，定理 8.10 が成り立つことを示す．▌

定理 8.10 の別証明 $x_1, x_2, \cdots, x_h$ を G の共役類の代表系として，(i, j) 成分が $\chi_i(x_j)/\sqrt{|C_G(x_j)|}$ なる行列 X を考える．定理 8.9 により，X は h 次正方行列である．第1直交関係は $XX^* = E_h$ $(X^* = {}^t\overline{X})$ を示す．よって $X^*X = E_h$ であるが，これが第2直交関係である．▌

例 8.10 正 2 面体群 D_{2n} の既約表現

$$D_{2n}:\ a^n = b^2 = 1, \qquad b^{-1}ab = a^{-1}$$

とする．D_{2n} の共役類の代表系は，

n=偶数のとき，1, $a^i\,(1 \leqq i \leqq n/2)$, b, ab　計 $n/2+3$ 個，

n=奇数のとき，1, $a^i\,(1 \leqq i \leqq (n-1)/2)$, b　計 $(n-1)/2+2$ 個

であることが簡単な計算によってわかる．また，D_{2n} の交換子群は，a^2 で生成される巡回部分群 $\langle a^2 \rangle$ である．したがって定理 8.4 により，D_{2n} の 1 次(既約)表現 (=1 次指標) の数は，

n=偶数のとき，$[D_{2n}:\langle a^2\rangle]=4$,

n=奇数のとき，$[D_{2n}:\langle a^2\rangle]=2$　($\langle a^2\rangle=\langle a\rangle$ に注意)

である．これらを具体的に与えると，次のようになる：

n が偶数のとき，$D_{2n}/\langle a^2\rangle$ は (2, 2) 型の Abel 群で $D_{2n}/\langle a^2\rangle=\langle \bar{a}\rangle \otimes \langle \bar{b}\rangle$ ($\bar{a}, \bar{b}$ は，a, b の $D_{2n}/\langle a^2\rangle$ への自然準同型の像) であるから，

$$\begin{array}{llll} a \longmapsto 1, & b \longmapsto 1 & (\text{恒等表現}) & \langle a, b\rangle = D_{2n}, \\ a \longmapsto 1, & b \longmapsto -1 & & \langle a\rangle, \\ a \longmapsto -1, & b \longmapsto 1 & & \langle a^2, b\rangle, \\ a \longmapsto -1, & b \longmapsto -1 & & \langle a^2, ab\rangle \end{array}$$

によって D_{2n} の 4 個の 1 次指標が得られる．ここで最後に書いてあるのは，それぞれの表現の核である．

n が奇数のとき，$D_{2n}/\langle a^2\rangle$ は位数 2 の巡回群で $\bar{b}$ がその生成元であるから，

$$\begin{array}{llll} a \longmapsto 1, & b \longmapsto 1 & (\text{恒等表現}) & \langle a, b\rangle = D_{2n}, \\ a \longmapsto 1, & b \longmapsto -1 & & \langle a\rangle \end{array}$$

が，D_{2n} の 2 個の 1 次表現である．さて，例 8.3 において各整数 k に対して

$$R_k'(a) = \begin{bmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{bmatrix}, \qquad R_k'(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \omega = \cos\frac{2\pi}{n}+\sqrt{-1}\sin\frac{2\pi}{n}$$

なる 2 次の表現 R_k' を与えた．この表現の指標 χ_k は

$$\chi_k(a^i) = \omega^{ik}+\omega^{-ik}, \qquad \chi_k(a^ib) = 0$$

である．これを，例 8.3 において与えたもう一つの 2 次の表現

$$R_k(a)=\begin{bmatrix}\cos\dfrac{2k\pi}{n} & -\sin\dfrac{2k\pi}{n}\\ \sin\dfrac{2k\pi}{n} & \cos\dfrac{2k\pi}{n}\end{bmatrix},\qquad R_k(b)=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$$

の指標と比較すると，それらは一致することがわかるから，定理8.7により，R_k と R_k' は同型な表現である．さて，χ_k の内積 (χ_k, χ_k) を計算して見よう：

$$\begin{aligned}(\chi_k,\chi_k)&=\frac{1}{2n}\sum_{x\in D_{2n}}\chi_k(x)\overline{\chi_k(x)}\\ &=\frac{1}{2n}\sum_{i=0}^{n-1}(\omega^{ik}+\omega^{-ik})\overline{(\omega^{ik}+\omega^{-ik})}\\ &=\frac{1}{2n}\sum_{i=0}^{n-1}(\omega^{ik}+\omega^{-ik})(\omega^{-ik}+\omega^{ik})\\ &=\frac{1}{2n}\sum_{i=0}^{n-1}(1+\omega^{2ik}+\omega^{-2ik}+1)\\ &=\frac{1}{2n}\left(2n+\sum_{i=0}^{n-1}\omega^{2ik}+\sum_{i=0}^{n-1}\omega^{-2ik}\right).\end{aligned}$$

ところで，よく知られているように

$$\sum_{i=0}^{n-1}\omega^{2ik}=\begin{cases}0 & \left(k\neq\dfrac{n}{2}\right),\\ n & \left(k=\dfrac{n}{2}\right)\end{cases}$$

であるから，

$$(\chi_k,\chi_k)=\begin{cases}1 & \left(k\neq\dfrac{n}{2}\right),\\ 2 & \left(k=\dfrac{n}{2}\right)\end{cases}$$

を得る．したがって定理8.8により

　　$k\neq n/2$ のとき，R_k' は D_{2n} の既約表現

であることがわかる．また $k\equiv\pm k'\ (\mathrm{mod}\ n)$ ならば，明らかに R_k' と $R_{k'}'$ の指標は一致する．しかも

　　n＝偶数のとき，R_1', R_2', $\cdots$, $R_{n/2-1}'$,

　　n＝奇数のとき，R_1', R_2', $\cdots$, $R_{(n-1)/2}'$

の指標は異なるから，定理 8.7 により，これらの表現は同型ではない．そこで，最初に与えた D_{2n} の共役類の数と比較すると，定理 8.9 により，D_{2n} の既約表現は

n=偶数のとき，四つの 1 次表現と $n/2-1$ 個の 2 次表現 R_k',

n=奇数のとき，二つの 1 次表現と $(n-1)/2$ 個の 2 次表現 R_k'

からなることがわかった．

問 8.10 例 8.4 で与えた Q_{4n} の表現を用いて，Q_{4n} の互いに同型でないすべての既約表現を与えよ．——

有限群 G が与えられたとき，

(α) G の共役類を決定すること（各共役類の代表元を求めること），

(β) G の互いに同型でないすべての既約表現（行列表現あるいは表現空間）を求めること，

(γ) G のすべての既約指標を求めること

は，有限群の表現論の主要な問題である．これらの問題とくに (β), (γ) については，重要な群（有限体上の Lie 型の群など）に対しても現在のところ満足すべき結果が得られていない．また上の例 8.10 では，D_{2n} の既約表現を与えているが，一般には (γ) が比較的簡単に解決されても，(β) は非常に難しいのが通例である．

指標表 (character table)　一般に，G を有限群，$x_1, x_2, \cdots, x_h$ を G の共役類の代表系，$\chi_1, \chi_2, \cdots, \chi_h$ を G の既約指標の全体とするとき，$\chi_i(x_j)$ を (i, j) 成分にする h 次行列を G の指標表という．たとえば，正 2 面体群 D_{2n} の指標表はつぎのようになる：

n が奇数のとき，

	1	$a^i\left(1\leqq i\leqq\frac{n-1}{2}\right)$	b	
ξ_0	1	1	1	(恒等指標)
ξ_1	1	1	-1	
χ_k	2	$\omega^{ik}+\omega^{-ik}$	0	$\left(1\leqq k\leqq\frac{n-1}{2}\right)$

n が偶数のとき，

	1	$a^i\left(1\leqq i\leqq \frac{n}{2}\right)$	b	ab	
ξ_0	1	1	1	1	(恒等指標)
ξ_1	1	1	-1	-1	
ξ_2	1	$(-1)^i$	1	-1	
ξ_3	1	$(-1)^i$	-1	1	
χ_k	2	$\omega^{ik}+\omega^{-ik}$	0	0	$\left(1\leqq k\leqq \frac{n}{2}-1\right)$

例 8.11　4 次対称群の既約指標　4 次対称群 $\mathfrak{S}_4$ の共役類の代表系は

$$(1),\quad (1\ 2),\quad (1\ 2)(3\ 4),\quad (1\ 2\ 3),\quad (1\ 2\ 3\ 4)$$

であり (定理 1.8), それぞれの共役類の元の数は

$$1,\quad 6,\quad 3,\quad 8,\quad 6$$

である (問 1.48, p. 37). $\mathfrak{S}_4$ の交換子群は交代群 $\mathfrak{A}_4$ であるから $\mathfrak{S}_4$ は二つの 1 次指標をもち, 一つは恒等指標, 他の一つは交代指標 (例 8.1) である. さて, $\mathfrak{S}_4$ の $\{1, 2, 3, 4\}$ の上の自然な作用から得られる置換表現の指標 χ を考える. χ の値は $\mathfrak{S}_4$ の各元の固定点の数に等しい (例 8.8) から,

$$\chi:\ 4,\ 2,\ 0,\ 1,\ 0$$

であることがわかる. この指標と恒等指標との内積を作ると,

$$\frac{1}{24}(4+2\times 6+0\times 3+1\times 8+0\times 6)=1$$

であるから, χ は,

$$\chi = 1_{\mathfrak{S}_4}+\chi'$$

の形に分解され, 指標 χ' の値は

$$\chi':\ 3,\ 1,\ -1,\ 0,\ -1$$

である. χ' の内積を作ると,

$$(\chi', \chi')=\frac{1}{24}(9\times 1+1\times 6+1\times 3+0\times 8+1\times 6)=1$$

であるから, χ' は $\mathfrak{S}_4$ の既約指標である (定理 8.8). ところで, χ' と $\mathfrak{S}_4$ の交代指標のテンソル積の指標は (8.27) により,

$$3,\quad -1,\quad -1,\quad 0,\quad 1$$

となり, 内積を計算すると, これも $\mathfrak{S}_4$ の既約指標であることがわかる. いまま

でに，$\mathfrak{S}_4$ の5個の既約指標のうち4個が得られ

(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)
1	1	1	1	1
1	−1	1	1	−1
3	1	−1	0	−1
3	−1	−1	0	1

であるが，最後の指標の値を

$$x_1,\quad x_2,\quad x_3,\quad x_4,\quad x_5$$

とすると，これらは(たとえば)第2直交関係から求められる．たとえば

$$1^2+1^2+3^2+3^2+x_1{}^2=24$$

から，$x_1=2$，第1列と第2列の直交性から

$$1\times1+1\times(-1)+3\times1+3\times(-1)+2x_2=0,\qquad \therefore\quad x_2=0.$$

同様にして $x_3=2$，$x_4=-1$，$x_5=0$ を得る．以上により $\mathfrak{S}_4$ の指標表は，

(1)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2 3 4)	
1	1	1	1	1	(恒等指標)
1	−1	1	1	−1	(交代指標)
3	1	−1	0	−1	
3	−1	−1	0	1	
2	0	2	−1	0	

となる．なお，最後に求めた2次の指標は，$V=\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ とするとき，

$$\mathfrak{S}_4 \rhd V,\qquad \mathfrak{S}_4/V\simeq D_6\,(\simeq\mathfrak{S}_3)$$

であり，D_6 の2次の既約指標を $\mathfrak{S}_4$ の既約指標と見たものである(§8.2, b)で説明した群とその剰余群の表現の関係に注意)．

問 8.11　4次交代群 $\mathfrak{A}_4$ の指標表は，

(1)	(1 2)(3 4)	(1 2 3)	(1 3 2)
1	1	1	1
1	1	ω	ω^2
1	1	ω^2	ω
3	−1	0	0

$$\omega=\cos\frac{2\pi}{3}+\sqrt{-1}\sin\frac{2\pi}{3}$$

となることを示せ．

問 8.12　有限群 G の任意の既約表現と任意の1次表現のテンソル積は，G の既約表現であることを示せ．［ヒント］例8.11において第2の3次指標を求めるときにこの原理を用いているから，それを参考にせよ．

問 8.13　$G=G_1\otimes G_2$ とする．ρ_1, ρ_2 をそれぞれ G_1, G_2 の既約表現とするとき，$(x_1, x_2)\mapsto \rho_1(x_1)\otimes\rho_2(x_2)$ $(x_i \in G_i)$ は G の既約表現であることを示せ．逆に，G の既約表現は，すべてこのようにして得られることを示せ．［ヒント］指標を考えよ．——

一般に与えられた群の既約表現や既約指標を求めるもっとも有力な手段は，つぎの§8.4で述べる誘導表現や誘導指標を計算することである．例8.2のすぐ後で注意したように，置換表現は誘導表現の特別の場合であるから，上の例8.11でもすでに誘導表現は暗々裡のうちに用いられているわけである．

c) 既約表現の次数

有限群 G の既約表現の次数についてつぎの著しい結果が知られている：

定理 8.11　有限群の複素数体上の既約表現の次数は，群の位数の約数である．——

この定理の証明は，指標の第1直交関係と，つぎのような数

$$\frac{|K|\chi(x)}{\chi(1)} \qquad (\chi \text{ は既約指標，} K \text{ は共役類，} x\in K)$$

の数論的性質に基づく．

定理 8.12　χ を G の既約指標，K を G の共役類とするとき，$|K|\chi(x)/\chi(1)$ $(x\in K)$ は代数的整数である．

注意　$|K|\chi(x)/\chi(1)$ なる数の数論的性質は，指標の理論（とくにモジュラー表現論）やその有限群論への応用において極めて重要である．定理8.12は，この数の一つの性質である．この項c)およびつぎの項d)において，定理8.12は有効に応用されるであろう．

さて，定理8.11, 8.12を証明する前に，代数的整数について簡単に説明しておこう．複素数 α は，最高次の係数が1の整数係数の多項式の根であるとき，**代数的整数**とよばれる．つぎの補題8.3は大切である．

補題 8.3　(i)　二つの代数的整数の和，差，積は代数的整数である．いいかえると，代数的整数の全体は，複素数体の部分環である．

(ii)　有理数が代数的整数であるためには，それが整数であることが必要十分である．——

この補題の証明は，それほど難しくはないので読者自ら試みられたい (本選書“体と Galois 理論”あるいは岩波講座基礎数学“数論”を参照)．

例 8.12　(i)　整数 $0, \pm 1, \pm 2, \cdots$ は代数的整数である．

(ii)　1 の巾根 ($\omega^m=1$ なる数 ω) は代数的整数である．群指標の値は，1 の巾根の和であるから (補題 8.2 の証明参照)，補題 8.3 の (i) により代数的整数である．

(iii)　整数を成分とする正方行列の固有値は代数的整数である．

定理 8.12 の証明　(ρ, V) を G の $\boldsymbol{C}$ 上の既約表現，χ をその指標とする．$K_1, K_2, \cdots, K_h$ を G の共役類の全体，$\hat{K}_i$ を §8.1, c) におけるように，$\hat{K}_i=\sum_{x\in K_i} x$ なる群環 $\boldsymbol{C}[G]$ の元とするとき，

$$\hat{K}_i\hat{K}_j = \sum_{k=1}^{h} a_{ijk}\hat{K}_k \qquad (a_{ijk}\in \boldsymbol{Z})$$

である．ρ を §8.1, c) で述べたように群環 $\boldsymbol{C}[G]$ の表現に拡張すると，

$$(*)\qquad \rho(\hat{K}_i)\rho(\hat{K}_j) = \rho(\hat{K}_i\hat{K}_j) = \sum_{k=1}^{h} a_{ijk}\rho(\hat{K}_k)$$

である．ところで，簡単な計算により

$$\rho(\hat{K}_i)\rho(x) = \rho(x)\rho(\hat{K}_i) \qquad (\forall x\in G)$$

であるから，Schur の補題 8.1 により $\rho(\hat{K}_i)$ はスカラー行列 $\alpha 1_V$ であるが，$\rho(\hat{K}_i)=\alpha 1_V$ の両辺のトレースをとれば，

$$\alpha = \frac{|K_i|\chi(x_i)}{\chi(1)} \qquad (x_i\in K_i)$$

を得る．そこで

$$\omega(K_i) = \frac{|K_i|\chi(x_i)}{\chi(1)} \qquad (x_i\in K_i)$$

とおくと，$(*)$ から

$$(8.35)\qquad \omega(K_i)\omega(K_j) = \sum_{k=1}^{h} a_{ijk}\omega(K_k)$$

を得るが，i をとめて j, k を 1 から h まで動かせば，(8.35) は $\omega(K_i)$ が整数成分の h 次行列 (a_{ijk}) の固有値であることを示す．したがって，例 8.12 の (iii) に

より $\omega(K_i)$ は代数的整数である．これが定理 8.12 の主張である．▌

定理 8.11 の証明　χ を G の既約指標，$K_1, K_2, \cdots, K_h$ を G の共役類の全体，$K_i \ni x_i$ とする．第1直交関係により

$$\sum_{i=1}^{h} |K_i|\chi(x_i)\overline{\chi(x_i)} = |G|$$

である．この両辺を $\chi(1)$ で割ると

$$\sum_{i=1}^{h} \frac{|K_i|\chi(x_i)}{\chi(1)}\overline{\chi(x_i)} = \frac{|G|}{\chi(1)}$$

となるが，左辺は定理 8.12，補題 8.3，例 8.12 により代数的整数であり，よって右辺の有理数 $|G|/\chi(1)$ は補題 8.3 の (ii) により整数でなければならない．すなわち $\chi(1)$ は $|G|$ を割る．▌

定理 8.11 はつぎのように少し一般化される．後にこれをさらに一般化するであろう (§8.4，c) 定理 8.20)．

定理 8.13　有限群 G の既約表現の次数は $[G:Z(G)]$ ($Z(G)$ は G の中心) を割る．

証明 (Glauberman)　χ を G の既約指標，$K_1, K_2, \cdots, K_h$ を G の共役類の全体，$K_i \ni x_i$ とする．まず，$Z(G) \ni z$ ならば zK_i ($1 \leqq i \leqq h$) も G の共役類であることに注意する．すなわち，$Z(G)$ は共役類の集合 $\{K_1, K_2, \cdots, K_h\}$ の上に $K_i \mapsto zK_i$ ($z \in Z(G)$) によって作用する．場合を二つに分けよう：

(α)　χ が忠実の場合．このとき，

$$(*) \qquad zK_i = K_i, \quad Z(G) \ni z \neq 1 \Longrightarrow \chi(x_i) = 0 \quad (x_i \in K_i)$$

である．実際，

$$\begin{aligned} \chi(x_i) &= \chi(zx_i) && (zK_i = K_i \text{ による}) \\ &= \frac{\chi(z)\chi(x_i)}{\chi(1)} && (\text{補題 } 8.2 \text{ の (v)}) \end{aligned}$$

であるから，$\chi(x_i) \neq 0$ ならば，$\chi(1) = \chi(z)$ すなわち $1 \neq z \in \operatorname{Ker}\chi$ (補題 8.2 の (iv)) となり，χ の忠実性に反する．$Z(G)$ の $\{K_1, K_2, \cdots, K_h\}$ への作用による軌道で長さ (＝含まれる共役類の数) が $|Z(G)|$ に等しいもの全体を考え，そのような軌道の代表系を $K_1, K_2, \cdots, K_s$ とする．このとき，

$$\{zK_i \mid z \in Z(G),\ 1 \leqq i \leqq s\}$$

は，$zK \neq K$ $(1 \neq \forall z \in Z(G))$ なる共役類の全体であるから，上の(＊)と第1直交関係により

$$|G| = \sum_{i=1}^{s} \sum_{z \in Z(G)} |K_i| \chi(zx_i) \overline{\chi(zx_i)}$$

$$= \sum_{i=1}^{s} \sum_{z \in Z(G)} |K_i| \frac{\chi(z)}{\chi(1)} \frac{\overline{\chi(z)}}{\chi(1)} \chi(x_i) \overline{\chi(x_i)} \qquad \text{(補題 8.2 の (v))}$$

$$= |Z(G)| \sum_{i=1}^{s} |K_i| \chi(x_i) \overline{\chi(x_i)} \qquad \left(\left| \frac{\chi(z)}{\chi(1)} \right| = 1 \right),$$

$$\therefore \quad \frac{[G:Z(G)]}{\chi(1)} = \sum_{i=1}^{s} \frac{|K_i| \chi(x_i)}{\chi(1)} \overline{\chi(x_i)}.$$

この右辺は，定理 8.12 により代数的整数であるから，左辺は整数となり，$\chi(1) \mid [G:Z(G)]$ である．

(β) χ が忠実でない場合．$N = \mathrm{Ker}\,\chi$ とし，$\bar{G} = G/N$ とおく．$Z(\bar{G}) \supseteq \overline{Z(G)} = Z(G)N/N$ であるから，$[\bar{G}:Z(\bar{G})] \mid [\bar{G}:\overline{Z(G)}]$．よって $[\bar{G}:Z(\bar{G})] \mid [G:Z(G)]$ である．一方 χ は $\bar{G}$ の忠実な既約指標であるから，(α) により $\chi(1) \mid [\bar{G}:Z(\bar{G})]$．よって $\chi(1) \mid [G:Z(G)]$． ▌

定理 8.12 の証明における (8.35) は，いろいろな形で応用される (§8.8, a) 参照)．ここでは，(8.35) を変形して既約指標の満たす一つの関係式を導こう．$G \ni x$ に対して K_x により x を含む共役類を表わすとき，既約指標 χ はつぎの等式を満たす：

(8.36) $$|K_b| \chi(a) \chi(b) = \chi(1) \sum_{x \in K_b} \chi(ax) \qquad (\forall a, b \in G).$$

実際，(8.35) より

$$\frac{|K_a| \chi(a)}{\chi(1)} \frac{|K_b| \chi(b)}{\chi(1)} = \sum_c a_c \frac{|K_c| \chi(c)}{\chi(1)}.$$

ここで c は G の共役類の代表系を走り，a_c は $xy = c$ なる $(x, y) \in K_a \times K_b$ の個数である (§8.1, c) 参照)．この式の右辺を変形しよう：

$$\sum_c a_c |K_c| \chi(c) = \sum_{(x,y) \in K_a \times K_b} \chi(xy)$$

$$= \frac{1}{|C_G(a)||C_G(b)|} \sum_{(u,v) \in G \times G} \chi(u^{-1}auv^{-1}bv)$$

$$= \frac{1}{|C_G(a)||C_G(b)|} \sum_{(u,v) \in G \times G} \chi(a(vu^{-1})^{-1}bvu^{-1})$$

$$= \frac{|G|}{|C_G(a)||C_G(b)|}\sum_{u \in G}\chi(au^{-1}bu)$$

$$= \frac{|G|}{|C_G(a)|}\sum_{x \in K_b}\chi(ax).$$

これと上の式を比べて (8.36) を得る.

問 8.14　(i)　φ, ψ を (8.36) を満たす類関数で $\varphi(1) \neq 0$, $\psi(1) \neq 0$ とするとき, $(\varphi(x)/\varphi(1))(\varphi, \psi) = (\psi(x)/\psi(1))(\psi, \varphi)$ を示せ.

(ii)　類関数 χ が (8.36), $\chi(1)>0$, $(\chi, \chi)=1$, $\overline{\chi(x)}=\chi(x^{-1})$ $(\forall x \in G)$ を満たすならば, χ は G の既約指標であることを示せ.

d) Burnside によるいくつかの定理

前項に引き続き, 直交関係のほかに指標の数論的性質を利用して Burnside により得られたいくつかの結果を述べる.

最初に, この項で用いられる円分体の簡単な性質を説明しよう. $\boldsymbol{Q}$ を有理数体, ω を 1 の原始 n 乗根とする. $\boldsymbol{Q}(\omega)$ を $\boldsymbol{Q}$ に ω を添加した体すなわち有理数係数の 1 変数有理式 $R(X)$ に対して $R(\omega)$ なる形の数全体からなる体とする. このような体を**円分体**あるいは**円体**という. このときつぎが成り立つ:

(8.37)　$(n, m)=1$ なるすべての整数 m に対して $R(\omega)=R(\omega^m)$ ならば, $R(\omega)$ は有理数である.

$m \equiv m' \pmod n$ ならば, 明らかに $R(\omega^m)=R(\omega^{m'})$ であるから, (8.37) において m を $1 \leqq m \leqq n-1$ なるものに限ってもよい. また $\omega^{-1}=\overline{\omega}$ であるから

$$R(\omega^{-1}) = \overline{R(\omega)}$$

である. さらに

(8.38)　$\boldsymbol{Q}(\omega) \ni R(\omega)$ が代数的整数ならば, $R(\omega^m)$ $((n, m)=1)$ も代数的整数である.

注意　(8.37), (8.38) は, 円分体 $\boldsymbol{Q}(\omega)$ の Galois 理論の簡単な帰結である. すなわち, $\boldsymbol{Q}(\omega)/\boldsymbol{Q}$ は Galois 拡大であり, その Galois 群は

$$\sigma_m(\omega) = \omega^m \qquad (1 \leqq m \leqq n-1,\ (m, n)=1)$$

なる $\boldsymbol{Q}(\omega)$ の自己同型 σ_m からなるという事実の直接の結果である. したがって (8.37), (8.38) の証明は, 本選書の“体と Galois 理論”を参照されたい.

補題 8.4　G を位数 n の群, χ を G の指標とする. このとき,

$$\prod_{(k, n)=1}\chi(x^k) \in \boldsymbol{Z} \qquad (x \in G)$$

である．ここで $\prod_{(k,n)=1}$ は $(k,n)=1$, $1\leqq k\leqq n-1$ なるすべての整数 k についての積を表わす．

証明　ρ を指標 χ をもつ表現，ω を 1 の原始 n 乗根とする．$\rho(x)$ $(x\in G)$ の固有値を $\omega_1, \omega_2, \cdots, \omega_t$ $(t=\chi(1)=\deg\rho)$ とするとき，$\omega_i=\omega^{a_i}$ $(a_i\in \boldsymbol{Z})$ と書けるから，

$$\chi(x^k)=\omega^{ka_1}+\omega^{ka_2}+\cdots+\omega^{ka_t}\in \boldsymbol{Q}(\omega)$$

である．また，$(m,n)=1$ とすると，

$$\prod_{(k,n)=1}(\omega^{ka_1}+\cdots+\omega^{ka_t})=\prod_{(k,n)=1}(\omega^{mka_1}+\cdots+\omega^{mka_t})$$

である．これは，k が n と素な整数の $\bmod n$ での代表系を走るとき，mk もそうであることからでる．よって (8.37) により

$$\prod_{(k,n)=1}\chi(x^k)=\prod_{(k,n)=1}(\omega^{ka_1}+\cdots+\omega^{ka_t})\in \boldsymbol{Q}$$

を得るが，右辺は代数的整数であるから，左辺は整数でなければならない．▌

まず，補題 8.4 の応用として，つぎの定理を証明しよう．

定理 8.14 (Burnside)　χ を $\deg\chi>1$ なる G の既約指標とするとき，G の或る元 x に対して $\chi(x)=0$.

証明　G のすべての元 x に対して $\chi(x)\neq 0$ と仮定して矛盾を導こう．$G\ni x$, y に対して $\langle x\rangle=\langle y\rangle$ なる関係は同値関係である．S を一つの同値類とするとき，

$$(*)\qquad \sum_{s\in S}|\chi(s)|^2\geqq |S|$$

を示そう．$S\ni x$, x の位数を n とするとき，補題 8.4 を群 $\langle x\rangle$ に適用して

$$\prod_{s\in S}|\chi(s)|^2=\prod_{(k,n)=1}\chi(x^k)\overline{\chi(x^k)}\in \boldsymbol{Z}$$

である．よって $\chi(s)\neq 0$ より

$$\prod_{s\in S}|\chi(s)|^2\geqq 1$$

である．このとき，$(*)$ は有名な不等式

$$\frac{a_1+a_2+\cdots+a_n}{n}\geqq \sqrt[n]{a_1a_2\cdots a_n}\qquad (a_i>0)$$

からでる．さて，単位元を含まないすべての同値類 S を走らせると，$(*)$ から

$$\sum_{1\neq x\in G}|\chi(x)|^2\geqq |G|-1$$

を得るが，第1直交関係により

$$|G| = \chi(1)^2 + \sum_{1 \neq x \in G} |\chi(x)|^2 \geqq \chi(1)^2 + |G| - 1$$

となり，$\chi(1)^2 \leqq 1$ すなわち $\deg \chi = 1$ となり矛盾である．▌

補題 8.5　χ を G の既約指標，K を G の共役類とする．$(|K|, \chi(1)) = 1$ ならば，$K \ni x$ に対して $\chi(x) = 0$ または $|\chi(x)| = \chi(1)$.

証明　$(|K|, \chi(1)) = 1$ であるから，

$$a|K| + b\chi(1) = 1$$

なる $a, b \in \boldsymbol{Z}$ が存在する(例題1.2)．このとき，等式

$$\frac{a|K|\chi(x)}{\chi(1)} + b\chi(x) = \frac{\chi(x)}{\chi(1)}$$

において，左辺の第1項は代数的整数(定理8.12)，第2項は例8.12により代数的整数，よって $\chi(x)/\chi(1)$ も代数的整数である．このとき，(8.37), (8.38)により

$$\prod_{(k,n)=1} \frac{\chi(x^k)}{\chi(1)} \in \boldsymbol{Z}$$

となり，$a_k = \chi(x^k)/\chi(1)$ とおくとき，$\chi(x) \neq 0$ ならば，

(＊)　$$\prod_{(k,n)=1} |a_k| \geqq 1.$$

一方，補題8.2(の証明)より $|a_k| \leqq 1$ であるから，(＊)と比べて $|a_k| = 1$，とくに $|a_1| = |\chi(x)|/\chi(1) = 1$ を得る．▌

最後に，§7.2, c)で述べた Burnside の定理を証明しよう．それはつぎの定理の系である．

定理 8.15 (Burnside)　G の或る共役類 K の元の数が素数の巾($\neq 1$)ならば，G は単純群ではない．

証明　$|K| = p^c \neq 1$，$\chi_1, \chi_2, \cdots, \chi_h$ を G の既約指標の全体とする．ただし χ_1 は G の恒等指標とする．まず $|K| \neq 1$ より G は非可換群であることに注意する．$K \ni x$ とすると第2直交関係により

$$1 + \sum_{i=2}^{h} \chi_i(1)\chi_i(x) = 0$$

である．この式から或る $i > 1$ に対して $p \nmid \chi_i(1)$，$\chi_i(x) \neq 0$ がわかる．なぜならすべての $i > 1$ に対して $p \mid \chi_i(1)$ または $\chi_i(x) = 0$ ならば，等式

$$\frac{1}{p} = -\sum_{i=2}^{h} \frac{\chi_i(1)}{p} \chi_i(x)$$

の右辺は代数的整数であるから，$1/p$ が整数となり矛盾である(補題8.3の(ii)). $p \nmid \chi_i(1)$，$\chi_i(x) \neq 0$ としよう．このとき，補題8.5により $|\chi_i(x)| = \chi_i(1)$ である．χ_i は恒等指標ではないから，$G \neq \mathrm{Ker}\,\chi_i$．よって $\mathrm{Ker}\,\chi_i \neq 1$ ならば，$\mathrm{Ker}\,\chi_i$ は G の自明でない正規部分群となり G は単純群ではない．よって $\mathrm{Ker}\,\chi_i = 1$ すなわち χ_i は忠実としよう．ρ を χ_i に対応する表現とするとき，$|\chi_i(x)| = \chi_i(1)$ および補題8.2(の証明)により，$\rho(x)$ はスカラー変換となる．このとき χ_i の忠実性より x は G の中心 $Z(G)$ に含まれ，G が非可換であるから，$Z(G)$ が G の自明でない正規部分群となる．▌

定理8.16 (Burnside)　G の位数がちょうど二つの素数で割れるとき G は可解群である．

証明　$|G| = p^a q^b$ (p, q は異なる素数)とし，P を G の Sylow p 部分群とする．P の中心 $Z(P)$ は単位群ではないから(定理2.4, p.60)，$Z(P) \ni x \neq 1$ をとる．このとき $C_G(x) \supseteq P$，よって $[G : C_G(x)]$ は q の巾で p と素である．ところで，$[G : C_G(x)]$ ($= q$ の巾)は x を含む共役類の元の数であるから，定理8.15により，G は自明でない正規部分群 N をもつ．このとき，N および G/N は定理8.16の仮定を満たすか，あるいはその位数は素数巾である．したがって N および G/N は可解群と仮定してよい．したがって G も可解群である．▌

§8.4 誘導表現

本節では，G の部分群 H と，H の表現 (ρ, V) が与えられたとき，それから誘導表現とよばれる G の表現を構成する方法を述べる．最初の項 a) では，誘導表現を H の表現 (ρ, V) の行列表示を用いて定義するが，実は理論上‘環上のテンソル積’の概念を用いて (ρ, V) から誘導表現の表現空間を構成するのが望ましい．これについては本節の d), e) で述べるであろう．しかし，誘導表現や誘導指標の具体的計算のためには，(とくに初学者にとっては)行列表現による定義で十分なことが多い．b) では Frobenius 相互律について述べる．Frobenius 相互律は表現論において非常に大切である．§8.7–§8.8 で述べる表現論の有限群論への応用の殆どすべては，本質的には Frobenius 相互律の応用である．c) では有限群とその正規部分群の指標の関係に関する Clifford の定理を述べ，最後に単項表現について簡単にふれる．

a）誘導表現

G を有限群，H を G の部分群，(ρ, V) を H の（任意の）体 k 上の表現としよう．(ρ, V) の行列表示

$$R(h) = (r_{ij}(h)) \in GL(m, k) \qquad (h \in H,\ m = \deg \rho)$$

と，G の H による左剰余類分解

$$G = x_1H + x_2H + \cdots + x_nH \qquad (n = [G:H])$$

をとる．まず，つぎのように行列 $R(x)$ の定義域を H から G へ拡張する：

$$R^0(x) = \begin{cases} R(x) & (x \in H), \\ 0 & (x \notin H) \end{cases} \qquad (0 \text{ は } m \text{ 次零行列}).$$

そこで $G \ni x$ に対して

$$R^G(x) = (R^0(x_i^{-1}xx_j))$$

なる m 次小行列 $R^0(x_i^{-1}xx_j)$ を (i, j) 成分とする mn 次行列 $R^G(x)$ を作る．ここで各 i に対して $x_i^{-1}xx_j \in H$ なる j はただ一つしか存在しないから，各 i に対してただ一つの j を除いて $R^0(x_i^{-1}xx_j) = 0$ であることに注意してほしい．

さて，

$$x \longmapsto R^G(x) \in GL(mn, k) \qquad (x \in G)$$

が，G の行列表現を与えること，すなわち

$$R^G(xy) = R^G(x)R^G(y) \qquad (x, y \in G)$$

を示そう．それには，

$$(*) \qquad \sum_{k=1}^{n} R^0(x_i^{-1}xx_k)R^0(x_k^{-1}yx_j) = R^0(x_i^{-1}xyx_j)$$

を示せばよい．$x_i^{-1}xx_l \in H$ としよう．上に注意したように，このような l は $(i, x$ を与えたとき$)$ ただ一つである．したがって

$$\begin{aligned}(**) \qquad \sum_{k=1}^{n} R^0(x_i^{-1}xx_k)R^0(x_k^{-1}yx_j) &= R^0(x_i^{-1}xx_l)R^0(x_l^{-1}yx_j) \\ &= \begin{cases} R(x_i^{-1}xx_l)R(x_l^{-1}yx_j) & (x_l^{-1}yx_j \in H), \\ 0 & (x_l^{-1}yx_j \notin H) \end{cases} \\ &= \begin{cases} R(x_i^{-1}xyx_j) & (x_l^{-1}yx_j \in H), \\ 0 & (x_l^{-1}yx_j \notin H). \end{cases}\end{aligned}$$

一方，

$$x_i^{-1}xyx_j \in H \Longleftrightarrow x_l^{-1}yx_j \in H$$

であるから，

$$(***) \qquad R^0(x_i^{-1}xyx_j) = \begin{cases} R(x_i^{-1}xyx_j) & (x_l^{-1}yx_j \in H), \\ 0 & (x_l^{-1}yx_j \notin H). \end{cases}$$

よって(**)と(***)を比較して(*)を得る．すなわち，$x \mapsto R^G(x)$ は G の行列表現である．行列表現 R^G の構成は，

(α) G の左剰余類分解の代表系，

(β) H の表現 (ρ, V) の行列表示

に依存しているが，これらのとり方を変えても得られる行列表現は同値である．実際，$G=x_1'H+\cdots+x_n'H$, $x_ih_i=x_i'$ $(h_i \in H)$ とするとき，

$$S = \begin{bmatrix} R(h_1) & & & \\ & R(h_2) & & \\ & & \ddots & \\ & & & R(h_n) \end{bmatrix}$$

とおけば，$S^{-1}R^G(x)S$ $(x \in G)$ が代表系 $\{x_1', x_2', \cdots, x_n'\}$ から得られる行列表現である．また，(ρ, V) の行列表示

$$h \longmapsto T^{-1}R(h)T \qquad (h \in H,\ T \text{ は } m \text{ 次正則行列})$$

から上のようにして構成される G の行列表現は，

$$S = \begin{bmatrix} T & & & \\ & T & & \\ & & \ddots & \\ & & & T \end{bmatrix} \quad (n \text{ 個})$$

とおくとき，$S^{-1}R^G(x)S$ である．

G の部分群 H の表現から，上のようにして構成された G の(行列)表現 R^G を (ρ, V) の**誘導表現**という．

例 8.13 H を G の部分群とする．G の G/H への作用から得られる置換表現 $1_H{}^G(x)$ の行列表示は，$G=x_1H+\cdots+x_nH$ とするとき，その (i, j) 成分が $xx_iH=x_jH$ なるとき 1，そうでないときは 0 であるから，誘導表現の定義と比較すれば，$1_H{}^G(x)$ は H の恒等表現から得られる誘導表現にほかならない．——

(ρ, V) が H の複素数体上の表現であるとき，その誘導表現の指標を**誘導指標**という．$\boldsymbol{C}(H)$ を §8.2, c) におけるように H の上の複素数値関数全体からなる

線型空間としよう．$C(H)\ni f$, $G\ni x$ に対して

$$f^0(x)=\begin{cases} f(x) & (x\in H), \\ 0 & (x\notin H) \end{cases} \tag{8.39}$$

とおく．χ_ρ を H の C 上の表現 (ρ, V) の指標とすれば，誘導表現 $R^G(x)$ の定義からわかるように

$$\mathrm{tr}\,(R^G(x))=\sum_{i=1}^{n}\mathrm{tr}\,(R^0(x_i{}^{-1}xx_i))=\sum_{i=1}^{n}\chi_\rho{}^0(x_i{}^{-1}xx_i)$$

である．よって

$$\sum_{i=1}^{n}\chi_\rho{}^0(x_i{}^{-1}xx_i)=\frac{1}{|H|}\sum_{y\in G}\chi_\rho{}^0(y^{-1}xy)$$

に注意すれば，誘導表現 R^G の指標 $\chi_\rho{}^G$ は

$$\chi_\rho{}^G(x)=\frac{1}{|H|}\sum_{y\in G}\chi_\rho{}^0(y^{-1}xy) \tag{8.40}$$

となる．この式は，R^G の指標が H の表現 ρ の指標 χ_ρ によって定まることを示しているから，(複素数体上の表現の場合には) (8.40) からも R^G が G/H の代表系および (ρ, V) の行列表示のとり方に依存せずに (同型を無視して) 定まることがわかる (定理 8.7)．また，(8.40) から

$$x \text{ が } H \text{ の元と共役でない} \Longrightarrow \chi_\rho{}^G(x)=0$$

である．

例 8.14　5次交代群の既約指標　5次交代群 $\mathfrak{A}_5$ の指標表はつぎのようになる：

	(1)	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 3 5 2 4)
	1	15	20	12	12
χ_0	1	1	1	1	1
χ_1	4	0	1	-1	-1
χ_2	5	1	-1	0	0
χ_3	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_4	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

ここで，第1行は共役類の代表系，第2行は各共役類の元の数，第3行以下が

既約指標の値を表わす.

最初に，交代群の共役類についてつぎのことを注意しておこう：K を n 次対称群 $\mathfrak{S}_n$ の共役類で $K\subseteqq\mathfrak{A}_n$ なるものとする．$K\ni x$ のとき，

(α) $C_{\mathfrak{S}_n}(x)\subsetneqq\mathfrak{A}_n$ ならば，K は $\mathfrak{A}_n$ の共役類でもある.

(β) $C_{\mathfrak{S}_n}(x)\subseteqq\mathfrak{A}_n$ ならば，K は $\mathfrak{A}_n$ において同じ個数の元からなる二つの共役類に分れ，$\mathfrak{S}_n-\mathfrak{A}_n\ni y$ とするとき，x と yxy^{-1} がそれらの代表元である.

(α), (β) の証明は，簡単であるから読者にまかせる.

まず，(α), (β) を用いて $\mathfrak{A}_5$ の共役類の代表元を求めよう．$\mathfrak{A}_5$ に含まれる $\mathfrak{S}_5$ の共役類の代表と，各共役類の元の数は

$$\begin{array}{cccc}(1) & (1\ 2)(3\ 4) & (1\ 2\ 3) & (1\ 2\ 3\ 4\ 5)\\ 1 & 15 & 20 & 24\end{array}$$

である (定理1.8, 問1.48)．(1 2)(3 4), (1 2 3) は奇置換と交換可能であるから，上の (α) によりそれらを含む $\mathfrak{S}_5$ の共役類は $\mathfrak{A}_5$ でも共役類である．しかし，$C_{\mathfrak{S}_5}((1\ 2\ 3\ 4\ 5))=\langle(1\ 2\ 3\ 4\ 5)\rangle\subseteqq\mathfrak{A}_5$ であるから，(β) により (1 2 3 4 5) を含む $\mathfrak{S}_5$ の共役類は $\mathfrak{A}_5$ で同じ個数の元からなる二つの共役類に分れる．(2 3 5 4)·(1 2 3 4 5)(2 3 5 4)$^{-1}$=(1 3 5 2 4) であるから，(1 2 3 4 5) と (1 3 5 2 4) は $\mathfrak{A}_5$ で共役ではない．以上により上の指標表の第1行と第2行が得られる．$\mathfrak{A}_5$ の既約指標を求めよう．上の表で χ_0 は恒等指標である．χ_1 は $\mathfrak{A}_5$ の $\{1,2,3,4,5\}$ の上への自然な作用から得られる置換表現の指標(この値は $\mathfrak{A}_5$ の元の固定点の数に等しい)から，恒等指標を引いたものである (例8.11参照)．5次指標 χ_2 を求めよう．以下，$\mathfrak{A}_5=G$ と書き，H を $\{1,2,3,4\}$ の上の交代群として G の部分群と考える:

$$H=\langle(1\ 2\ 3),(1\ 2)(3\ 4)\rangle\subseteqq G.$$

ε を1の原始3乗根とするとき，H は

$$\varphi((1\ 2)(3\ 4))=1,\qquad \varphi((1\ 2\ 3))=\varepsilon$$

なる1次指標 φ をもつ (問8.11)．φ の G への誘導指標 φ^G を計算しよう．(1 2 3 4 5), (1 3 5 2 4) は H の元と共役ではないから，

$$\varphi^G((1\ 2\ 3\ 4\ 5))=\varphi^G((1\ 3\ 5\ 2\ 4))=0$$

である．$y^{-1}(1\ 2)(3\ 4)y\in H$ $(y\in G)$ とすると，

$$(*)\qquad y^{-1}(1\ 2)(3\ 4)y=(1\ 2)(3\ 4),\ \ (1\ 3)(2\ 4),\ \ (1\ 4)(2\ 3)$$

であるが,

$$C_G((1\ 2)(3\ 4)) = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$
$$\therefore\quad |C_G((1\ 2)(3\ 4))| = 4$$

に注意すれば,（$*$）を満たす y は（（$*$）の右辺の各元に対して）それぞれ4個あることがわかる．よって $\varphi^G((1\ 2)(3\ 4))$ の値を (8.40) により計算すると

$$\varphi^G((1\ 2)(3\ 4)) = \frac{1}{12}(4+4+4) = 1$$

を得る．つぎに $y^{-1}(1\ 2\ 3)y \in H$ $(y \in G)$ とすると，$y^{-1}(1\ 2\ 3)y$ は，$V=\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ として

$$(1\ 2\ 3)V = \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}$$
$$(1\ 3\ 2)V = \{(1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4), (1\ 2\ 4)\}$$

なる8個の元の一つである．ところで $C_G((1\ 2\ 3)) = \langle(1\ 2\ 3)\rangle$ は位数3であるから，$y^{-1}(1\ 2\ 3)y$ が上の8個の元の一つとなる y は，それぞれ3個ずつ存在する．よって (8.40) により，

$$\begin{aligned}\varphi^G((1\ 2\ 3)) &= \frac{1}{12}(3\varepsilon+3\varepsilon+3\varepsilon+3\varepsilon+3\varepsilon^{-1}+3\varepsilon^{-1}+3\varepsilon^{-1}+3\varepsilon^{-1})\\ &= \varepsilon+\varepsilon^{-1}\\ &= -1\end{aligned}$$

となる．以上により φ^G の値は，

$$5,\quad 1,\quad -1,\quad 0,\quad 0$$

であることがわかった．そこで φ^G の内積を計算してみると $(\varphi^G, \varphi^G)=1$ であるから，定理8.8により φ^G は $\mathfrak{A}_5$ の既約指標であることがわかる．これが指標表における χ_2 である．つぎに，$H_1 = \langle(1\ 2\ 3\ 4\ 5), (2\ 5)(3\ 4)\rangle$ としよう．$((2\ 5)(3\ 4))^{-1}(1\ 2\ 3\ 4\ 5)((2\ 5)(3\ 4)) = (1\ 2\ 3\ 4\ 5)^{-1}$ であるから，H_1 は位数10の正2面体群である．したがって H_1 は

$$\psi((1\ 2\ 3\ 4\ 5)) = \omega+\omega^{-1} \qquad \left(\omega=\cos\frac{2\pi}{5}+\sqrt{-1}\sin\frac{2\pi}{5}\right),$$
$$\psi((1\ 2\ 3\ 4\ 5)^2) = \psi((1\ 3\ 5\ 2\ 4)) = \omega^2+\omega^{-2},$$
$$\psi((2\ 5)(3\ 4)) = 0$$

なる2次既約指標 ψ をもつ（例8.10）．上の φ^G の計算とまったく同様にして，

ψ^G の値は

$$12, \quad 0, \quad 0, \quad \omega+\omega^{-1}, \quad \omega^2+\omega^{-2}$$

であることがわかる．このとき，内積 (ψ^G, χ_1), (ψ^G, χ_2) を計算して

$$(\psi^G, \chi_1) = (\psi^G, \chi_2) = 1$$

であるから，

$$\psi^G = \chi_1+\chi_2+\xi$$

とおくと，ξ の値は

$$3, \quad -1, \quad 0, \quad -(\omega^2+\omega^{-2}), \quad -(\omega+\omega^{-1})$$

となり，内積 (ξ, ξ) を計算して ξ は G の既約指標であることがわかる．これが指標表における χ_3 である．同様にして H_1 のもう一つの 2 次指標

$$\psi'((1\ 2\ 3\ 4\ 5)) = \omega^2+\omega^{-2},$$
$$\psi'((1\ 3\ 5\ 2\ 4)) = \omega+\omega^{-1},$$
$$\psi'((2\ 5)(3\ 4)) = 0$$

の誘導指標 ψ'^G から，指標表における χ_4 が得られる．$\mathfrak{A}_5$ は 5 個の共役類をもつから，定理 8.9 により $\chi_0, \chi_1, \chi_2, \chi_3, \chi_4$ が $\mathfrak{A}_5$ のすべての既約指標を与える．

注意 一般に G の既約指標を部分群の既約指標の誘導指標を計算して求めるのに，G のどんな部分群に注目すべきかについて一般法則はない．しかし，G の可換部分群 A で

$$A \ni a \neq 1 \Longrightarrow C_G(a) = A$$

なるものの正規化群 $N_G(A)$ に注目し，その既約指標の誘導指標を計算するのは多くの場合に有効である．その理由は，そのような誘導指標の G の既約指標への分解について，或る種の法則性があることによる (§8.7, c) 参照)．上の例 8.14 の計算もこのような可換部分群 (V および $\langle(1\ 2\ 3\ 4\ 5)\rangle$) に注目していることに注意してほしい．

問 8.15 5 次対称群 $\mathfrak{S}_5$ の指標表はつぎのようになることを示せ：

(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)	(1 2 3)(4 5)	(1 2 3 4 5)
1	1	1	1	1	1	1
4	2	1	0	0	−1	−1
5	1	−1	−1	1	1	0
6	0	0	0	−2	0	1
5	−1	−1	1	1	−1	0
4	−2	1	0	0	1	−1
1	−1	1	−1	1	−1	1

［ヒント］ 4次指標の一つは，$\mathfrak{S}_5$ の自然な置換表現から恒等表現を取り除いて得られるもの．$a=(1\ 2\ 3\ 4\ 5)$，$b=(2\ 4\ 5\ 3)$ とおくと $b^{-1}ab=a^2$ で，$\langle a, b\rangle$ は位数20の部分群である．この部分群の1次指標の誘導指標を計算して $\mathfrak{S}_5$ の5次指標の一方と6次指標を得る．もう一つの4,5次指標は，既に得られたものと交代指標のテンソル積を作ればよい.) ——

なお，n 次対称群の既約指標，既約表現は知られている．これについては，岩波講座基礎数学“対称群と一般線型群の表現論”を参照されたい．

b）Frobenius 相互律

G を有限群，H を G の部分群とする．G 上で定義された複素数値関数の作る線型空間 $\boldsymbol{C}(G)$ の元 f に対して，f の定義域を H に制限すると，$\boldsymbol{C}(H)$ の元を得る．これを

$$f\,|\,H \quad \text{あるいは} \quad f_H$$

によって表わす．とくに χ が指標のとき，$\chi\,|\,H$ は χ を指標とする G の表現 ρ を H に制限して得られる H の表現の指標である．一方，$\boldsymbol{C}(H)\ni g$ に対して

$$g^G(x)=\frac{1}{|H|}\sum_{y\in G}g^0(y^{-1}xy) \tag{8.41}$$

(g^0 の定義は (8.39) 参照) とおくと，$g^G\in\boldsymbol{C}(G)$ を得る．g が H の指標であるとき，(8.40) により g^G は誘導指標である．$\boldsymbol{C}(G), \boldsymbol{C}(H)$ の上には，内積が定義されているが，それらをそれぞれ

$$(f, g)_G \quad (f, g\in\boldsymbol{C}(G)), \qquad (h, k)_H \quad (h, k\in\boldsymbol{C}(H))$$

と書く：

$$(f, g)_G=\frac{1}{|G|}\sum_{x\in G}f(x)\overline{g(x)}, \qquad (h, k)_H=\frac{1}{|H|}\sum_{y\in H}h(y)\overline{k(y)}.$$

また，$Cl(G), Cl(H)$ によって，それぞれ G, H 上の類関数全体の作る $\boldsymbol{C}(G)$，$\boldsymbol{C}(H)$ の部分空間を表わす．このとき

$$g\in Cl(H) \Longrightarrow g^G\in Cl(G)$$

である．つぎの定理は大切である．

定理 8.17（**Frobenius 相互律**） $Cl(G)\ni f$，$Cl(H)\ni g$ とするとき，

$$(f\,|\,H, g)_H=(f, g^G)_G$$

が成り立つ．

証明
$$(f, g^G)_G = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{g^G(x)}$$
$$= \frac{1}{|G|}\sum_{x\in G} f(x)\left(\frac{1}{|H|}\sum_{y\in G}\overline{g^0(y^{-1}xy)}\right)$$
$$= \frac{1}{|G||H|}\sum_{y^{-1}xy\in H} f(x)\overline{g(y^{-1}xy)}$$

ここで $\sum_{y^{-1}xy\in H}$ は $y^{-1}xy\in H$ なる G の元の順列 (x, y) のすべてを走る．このとき，

$$= \frac{1}{|G||H|}\sum_{\substack{y\in G\\ h\in H}} f(yhy^{-1})\overline{g(h)}$$
$$= \frac{1}{|G||H|}|G|\sum_{h\in H} f(h)\overline{g(h)} \qquad (f\in Cl(G) \text{ による})$$
$$= \frac{1}{|H|}\sum_{h\in H} f(h)\overline{g(h)}$$
$$= (f\,|\,H, g)_H. \qquad \blacksquare$$

一般に α を G の $\boldsymbol{C}$ 上の表現，β を G の $\boldsymbol{C}$ 上の既約表現とするとき，α を既約表現の直和に分解し，β と同型な表現が m 回現われるならば，m を α に含まれる β の重複度というのであった．χ_α, χ_β をそれぞれ α, β の指標とするとき，直交関係により

$$(\chi_\alpha, \chi_\beta) = (\alpha \text{ に含まれる } \beta \text{ の重複度})$$

である．このことに注意すると，定理 8.17 の特別の場合としてつぎの系を得る：

系 ρ を G の既約表現，η を G の部分群 H の既約表現とするとき，ρ の H への制限 $\rho\,|\,H$ に含まれる η の重複度は，誘導表現 η^G に含まれる ρ の重複度に等しい．——

この系を Frobenius 相互律ということもある．

例題 8.1 χ を G の Ω への作用から得られる置換表現の指標，t を (G, Ω) の軌道の数とすると，χ は G の恒等表現を重複度 t で含む．すなわち

$$(\chi, 1_G) = \frac{1}{|G|}\sum_{x\in G}\chi(x) = t$$

となり，固定点の数の平均は軌道の数に等しい．とくに (G, Ω) が可移ならば，χ は G の恒等表現をちょうど 1 回含む．

[証明]　$\Omega_1, \Omega_2, \cdots, \Omega_t$ を (G, Ω) の軌道とする．(G, Ω_i) の置換表現の指標を χ_i とすれば，$\chi=\chi_1+\chi_2+\cdots+\chi_t$ であるから (例 8.8, (8.29))，$(\chi_i, 1_G)=1$ を証明すればよい．すなわち (G, Ω) は始めから可移としてよい．このとき，(G, Ω) の1点の固定部分群を H とすれば，(G, Ω) の置換表現と $(G, G/H)$ の置換表現は同型であり，$(G, G/H)$ の指標は H の恒等指標 1_H の誘導指標 $1_H{}^G$ にほかならないから，$\chi=1_H{}^G$ である．そこで Frobenius 相互律を用いて

$$(\chi, 1_G)=(1_H{}^G, 1_G)=(1_H, 1_G\,|\,H)=(1_H, 1_H)=1$$

を得る．▌

例題 8.2　(G, Ω) を可移とする．(G, Ω) の置換表現の指標を χ とするとき，(G, Ω) が2重可移であるためには，$(\chi, \chi)=2$ であることが必要十分である．

[証明]　H を (G, Ω) の1点の固定部分群とするとき，(G, Ω) が2重可移であることは，(H, Ω) の軌道の数が2であることと同値である．(H, Ω) の指標は $\chi\,|\,H$ であるから，例題 8.1 を用いて，

$$(G, \Omega)=2\text{ 重可移} \Leftrightarrow (\chi\,|\,H, 1_H)=2$$

である．一方，$\chi=1_H{}^G$ に注意して

$$\begin{aligned}(\chi\,|\,H, 1_H)&=(\chi, 1_H{}^G) \qquad (\text{Frobenius 相互律})\\ &=(\chi, \chi)\end{aligned}$$

であるから，

$$(G, \Omega)=2\text{ 重可移} \Leftrightarrow (\chi, \chi)=2$$

を得る．▌

例題 8.1 により，(G, Ω) が可移のとき，$(\chi, 1_G)=1$ であるから，例題 8.2 により (G, Ω) が2重可移ならば，$\chi-1_G$ は G の既約指標であることがわかる．この原理は，例 8.11，例 8.14 において $\mathfrak{S}_4, \mathfrak{A}_5$ の既約指標を求めるときに用いられていることに注意．一般に n 次対称群，n 次交代群の自然な置換表現は2重可移であるから，それらは $n-1$ 次の既約表現をもつ．また $PSL(n, q)$ は，q 個の元からなる有限体上の $n-1$ 次元射影空間の上に2重可移に作用するから (例 2.5)，$PSL(n, q)$ は $q^{n-1}+q^{n-2}+\cdots+q$ 次の既約表現をもつ．

例 8.15　A を G の可換部分群とする．G の既約表現の次数は $[G:A]$ 以下である．実際，χ を G の既約指標，$\chi\,|\,A$ に含まれる A の既約指標 φ をとると，A は可換であるから φ は1次指標である (定理 8.2)．Frobenius 相互律により

χ は φ^G に含まれるから，$\chi(1) \leqq \varphi^G(1) = \varphi(1)[G:A] = [G:A]$ である．正 2 面体群，4 元数型の群の既約表現の次数は 1 または 2 である．なぜなら，これらは指数 2 の巡回部分群を含むからである．正 2 面体群，4 元数型の群についてのこれらの事実は例 8.10，問 8.10 によって，すでに知っていることであるが，最初に述べた原理を用いると既約表現の次数についての情報が早く得られるわけである．なお，A が G の可換正規部分群ならば，G の既約表現の次数は $[G:A]$ の約数であることを後に見るであろう（定理 8.20）．——

最後に φ^G $(\varphi \in \boldsymbol{C}(H))$ の定義 (8.41) からわかる簡単な事柄を述べよう．これらは，後にしばしば用いられる：

H, K は G の部分群とする．

(8.42)　（線型性）　$(\varphi+\psi)^G = \varphi^G+\psi^G, \quad (\alpha\varphi)^G = \alpha\varphi^G$

$$(\alpha \in \boldsymbol{C},\ \varphi, \psi \in \boldsymbol{C}(H)),$$

(8.43)　（結合則）　$H \subseteqq K, \quad \varphi \in \boldsymbol{C}(H)$　ならば　$(\varphi^K)^G = \varphi^G,$

(8.44)　$\varphi^G\psi = (\varphi\psi_H)^G \qquad (\varphi \in Cl(H),\ \psi \in \boldsymbol{C}(G)),$

(8.45)　$G = KH, \quad \varphi \in Cl(H)$　ならば　$\varphi^G \mid K = (\varphi \mid H \cap K)^K.$

(8.44) は，$Cl(G)$ を関数の和，積に関して環と見るとき，$\{\varphi^G \mid \varphi \in Cl(H)\}$ が $Cl(G)$ のイデアルであることを示している．

問 8.16　(8.42)-(8.45) を証明せよ．

c) Clifford の定理

N を G の正規部分群としよう．G の既約指標 χ を N に制限したとき，χ の N の既約指標への分解について重要な結果——定理 8.18——がある．それはつぎの簡単な補題 8.6 と Frobenius 相互律に基づくものである．$\boldsymbol{C}(N) \ni \theta,\ G \ni x$ に対して，

$$\theta^x(y) = \theta(xyx^{-1}) \qquad (y \in N)$$

によって，$\theta^x \in \boldsymbol{C}(N)$ を定義する．θ^x を θ の G に関する**共役**という．

補題 8.6　$G \triangleright N,\ \varphi, \psi \in Cl(N),\ x \in G$ とする．このとき，つぎの (i)-(iv) が成り立つ：

(i)　$\varphi^x \in Cl(N),$

(ii)　$(\varphi^x, \psi^x)_N = (\varphi, \psi)_N,$

(iii)　$\chi \in Cl(G) \Longrightarrow (\chi_N, \varphi^x)_N = (\chi_N, \varphi)_N,$

(iv)　φ が N の指標 $\Longrightarrow$ φ^x も N の指標.

証明　(i)　$N \ni y, z$ のとき,

$$\begin{aligned}\varphi^x(zyz^{-1}) &= \varphi(xzy(xz)^{-1}) \\ &= \varphi(z'xyx^{-1}z'^{-1}) \qquad (z'=xzx^{-1}\in N) \\ &= \varphi(xyx^{-1}) \qquad (\varphi\in Cl(N)\text{ による}) \\ &= \varphi^x(y),\end{aligned}$$

$$\therefore\quad \varphi^x \in Cl(N).$$

(ii)　$(\varphi^x, \psi^x)_N = \dfrac{1}{|N|}\sum_{y\in N}\varphi^x(y)\overline{\psi^x(y)} = \dfrac{1}{|N|}\sum_{y\in N}\varphi(xyx^{-1})\overline{\psi(xyx^{-1})}$

y が N のすべての元を走るとき, xyx^{-1} も N のすべての元を走るから,

$$= \frac{1}{|N|}\sum_{y\in N}\varphi(y)\overline{\psi(y)} = (\varphi, \psi)_N$$

である.

(iii)　$\chi\in Cl(G)$ ならば, ${\chi_N}^x=\chi_N$ である. よって (ii) により $(\chi_N, \varphi^x)=({\chi_N}^x, \varphi^x)=(\chi_N, \varphi)$ を得る.

(iv)　φ を N の行列表現 $y\mapsto R(y)$ $(y\in N)$ の指標とするとき, $y\mapsto R(xyx^{-1})$ $(y\in N)$ も N の表現であり, この指標が φ^x である. ▌

定理 8.18 (Clifford)　$G\rhd N$, χ を G の既約指標, θ を χ_N に含まれる N の既約指標, $\theta_1, \theta_2, \cdots, \theta_t$ を θ の G に関する異なる共役の全体とするとき,

$$(\sharp)\qquad \chi_N = e\sum_{i=1}^{t}\theta_i, \qquad e=(\chi_N, \theta)_N$$

である.

証明　$e=(\chi_N, \theta)$ とおくと, 補題 8.6 の (iii) により, $e=(\chi_N, \theta_i)_N$ $(i=1, 2, \cdots, t)$ である. よって ($\sharp$) を示すには, χ_N に含まれる N の既約指標が $\theta_1, \theta_2, \cdots, \theta_t$ に限ることをいえば十分である. Frobenius 相互律により, $e=(\chi_N, \theta)_N=(\chi, \theta^G)_G$ であるから,

$$\theta^G = e\chi + \cdots$$

である. N に制限して

$$(*)\qquad \theta^G\,|\,N = e\chi_N + \cdots$$

を得る. 一方, (8.41) により, $n\in N$ ならば

$$\begin{aligned}|N|\theta^G(n) &= \sum_{x\in G}\theta^0(xnx^{-1})\\ &= \sum_{x\in G}\theta(xnx^{-1}) \qquad (xnx^{-1}\in N \text{ に注意})\\ &= \sum_{x\in G}\theta^x(n).\end{aligned}$$

よって $\theta^G|N$ に含まれる N の既約指標は θ の共役に限る．このとき，(＊)から χ_N に含まれる N の既約指標も θ の共役に限ることがわかる．▌

以後，有限群 X の既約指標の全体を $\mathrm{Irr}\,(X)$ で表わすことにしよう．

$G\triangleright N$, $\mathrm{Irr}\,(N)\ni\theta$ に対して

$$I_G(\theta) = \{x\in G\,|\,\theta^x=\theta\}$$

とおくと，$I_G(\theta)$ は G の (N を含む) 部分群である．$I_G(\theta)$ を θ の G に関する**惰性群**という．容易にわかるように θ の G に関する異なる共役の数は，$[G:I_G(\theta)]$ に等しい．つぎの定理は大切である．

定理 8.19 $G\triangleright N$, $\mathrm{Irr}\,(N)\ni\theta$, $T=I_G(\theta)$ とする．また

$$\Theta_T = \{\psi\in\mathrm{Irr}\,(T)\,|\,(\psi,\theta^T)\neq 0\},\qquad \Theta_G = \{\chi\in\mathrm{Irr}\,(G)\,|\,(\chi,\theta^G)\neq 0\}$$

とおくとき，$\psi\mapsto\psi^G$ は Θ_T から Θ_G への全単射である．とくに $N=I_G(\theta)$ ならば，θ^G は G の既約指標である．

証明 $\Theta_T\ni\psi$, χ を ψ^G の既約成分 (ψ^G に含まれる G の既約指標) としよう．Frobenius 相互律により ψ は χ_T の既約成分である．$\theta_1,\theta_2,\cdots,\theta_t$ $(t=[G:T])$ を θ の G に関する異なる共役の全体とするとき，定理 8.18 により，

$$\chi_N = e\sum_{i=1}^{t}\theta_i,\qquad e=(\chi_N,\theta)$$

である．また θ の T に関する共役は θ に限るから，T,N に対して定理 8.18 を適用して

$$\psi_N = f\theta,\qquad f=(\psi_N,\theta)$$

である．ψ が χ_T の既約成分であることから $f\leqq e$ となるから，

$$et\theta(1) = \chi(1)\leqq\psi^G(1) = \psi(1)t = ft\theta(1)\leqq et\theta(1).$$

よってこの式の不等号はすべて等号となり，

$$(*)\qquad \chi(1)=\psi^G(1),\qquad (\chi_N,\theta)=e=f=(\psi_N,\theta)$$

を得る．前者から $\chi=\psi^G$ すなわち ψ^G は G の既約指標である．また $(\psi^G,\theta^G)=(\chi,\theta^G)=(\chi_N,\theta)\neq 0$ より，$\psi^G\in\Theta_G$ を得る．よって $\psi\mapsto\psi^G$ は Θ_T から Θ_G への

写像である．この写像が単射であることをみよう．$\varphi^G=\psi^G=\chi$ $(\varphi,\psi\in\Theta_T)$ とすると，(*)の第2式から $(\varphi_N,\theta)=(\psi_N,\theta)=(\chi_N,\theta)$ であるから，$\varphi\neq\psi$ ならば，$(\chi_N,\theta)\geqq((\varphi+\psi)_N,\theta)=2e$ となり矛盾である．よって $\psi\mapsto\psi^G$ $(\psi\in\Theta_T)$ は単射である．$\Theta_G\ni\chi$ としよう．$(\chi,\theta^G)=(\chi_N,\theta)\neq0$ より，$(\psi,\theta^T)=(\psi_N,\theta)\neq0$ なる χ_T の既約成分 ψ が存在する．$\psi\in\Theta_T$ である．Frobenius 相互律により $(\psi^G,\chi)=(\psi,\chi_T)\neq0$，また $\psi^G\in\Theta_G$ であるから $\psi^G=\chi$ でなければならない．すなわち $\psi\mapsto\psi^G$ $(\psi\in\Theta_T)$ は全射である．▌

定理 8.18-8.19 の応用を与えよう．最初は，既約表現の次数に関する定理 8.13 の一般化である．

定理 8.20 (Ito) A を G の可換正規部分群とするとき，G の既約表現の次数は $[G:A]$ を割る．

証明 $\mathrm{Irr}(G)\ni\chi$，λ を $(\chi_A,\lambda)\neq0$ なる A の既約指標とする．A は可換であるから，λ は1次指標である．また，定理 8.18-8.19 により

$$\chi=\psi^G,\qquad \psi_A=e\lambda\qquad(\exists\psi\in\mathrm{Irr}(I_G(\lambda)))$$

である．$T=I_G(\lambda)$，$\bar{T}=T/\mathrm{Ker}\,\psi$ とおくと，$\psi_A=e\lambda$ は，$\bar{A}\subseteqq Z(\bar{T})$ を示すから，

$$[\bar{T}:Z(\bar{T})]\mid[\bar{T}:\bar{A}]\mid[T:A]$$

である．ところで定理 8.13 により，$\psi(1)\mid[\bar{T}:Z(\bar{T})]$ であるから，$\psi(1)\mid[T:A]$ である．一方 $\chi=\psi^G$ より $\chi(1)=\psi(1)[G:T]$，よって $\chi(1)\mid[G:T][T:A]=[G:A]$ である．▌

G の既約表現 ρ が，真の部分群の或る(既約)表現の誘導表現であるとき，ρ を**非原始的**，そうでないとき，ρ を**原始的**という．また，ρ が G の或る部分群の1次表現の誘導表現であるとき，ρ は**単項表現**とよばれる．

補題 8.7 $G\triangleright N$，χ を G の原始的指標とするとき，つぎの(i)，(ii)が成り立つ：

(i) χ_N は N の或る既約指標の倍数である．すなわち $\chi_N=a\psi$ $(0<a\in\boldsymbol{Z},\ \psi\in\mathrm{Irr}(N))$．

(ii) N が Abel 群，χ が忠実 $\Longrightarrow N\subseteqq Z(G)$．

証明 (i) $\chi_N=e\sum_{i=1}^{t}\theta_i$ $(\theta_i\in\mathrm{Irr}(N))$ としよう(定理 8.18)．$t=1$ を示せばよい．定理 8.19 により

$$\chi=\psi^G\qquad(\exists\psi\in\mathrm{Irr}(I_G(\theta_1)))$$

であるが，χ は原始的だから，$G=I_G(\theta_1)$ すなわち $t=1$ でなければならない．

(ii) (i)により $\chi_N=e\theta\,(\theta\in\mathrm{Irr}\,(N))$ であるが，N は Abel 群だから θ は 1 次指標である．これと χ の忠実性から $N\subseteq Z(G)$ がわかる．▌

定理 8.21 有限巾零群の任意の既約表現は，単項表現である．

証明 最初につぎのことに注意する：

(＊) 非可換巾零群 G は，中心に含まれない可換正規部分群をもつ．

実際，G の昇中心列 $1\subsetneqq Z(G)\subsetneqq Z_2(G)\subseteqq\cdots$ において $Z_2(G)-Z(G)\ni a$ をとると，$\langle a, Z(G)\rangle$ は G の可換正規部分群で中心 $Z(G)$ には含まれない．さて，G を有限巾零群とするとき，G の部分群 K で

$$\chi=\psi^G \qquad (\exists\psi\in\mathrm{Irr}\,(K))$$

なるものが存在する ($G=K,\ \psi=\chi$ がそのような K, ψ の例である)．このような K の中で位数最小のものをとり，それを H とする．このとき，(8.43) により ψ は H の原始指標である．$\bar{H}=H/\mathrm{Ker}\,\psi$ とおくと，ψ は $\bar{H}$ の忠実な原始指標であるから補題 8.7 の (ii) により，$\bar{H}$ の可換正規部分群は $\bar{H}$ の中心に含まれなければならない．しかるに $\bar{H}$ は巾零群だから，上の(＊)により $\bar{H}$ は Abel 群となり，ψ は H の 1 次指標である．▌

問 8.17 有限群 G が

$$G=G_0\supsetneqq G_1\supsetneqq\cdots\supsetneqq G_{n-1}\supsetneqq G_n=1,$$
$$G\triangleright G_i,\qquad G_{i-1}/G_i=\text{巡回群}\qquad (i=1,\cdots,n)$$

なる部分群の列をもつとき，G を**超可解群**という．このとき，つぎの (i), (ii), (iii) を証明せよ：

(i) 超可解群の部分群，剰余群は超可解群である．

(ii) 非可換超可解群は，中心に含まれない可換正規部分群をもつ．

(iii) 超可解群の任意の既約表現は単項表現である．——

単項表現については，いろいろなことが知られている．たとえば“任意の既約表現が単項表現であるような有限群は可解群である (竹田の定理)”がある (逆は成立しない)．この定理の証明はそれ程難しいものではないが，本講では応用の機会がないので省略する．興味のある読者は，秋月，鈴木：代数 II (岩波全書) を参照されたい．

問 8.18 4 次対称群の任意の既約表現は単項表現であることを確かめよ．

問 8.19　$SL(2,3)$（可解群！）は2次既約表現をもつことを示し，これは単項表現ではないことを示せ．

d）環上のテンソル積

この項 d) では，環上のテンソル積について述べる．つぎの項 e) ではその応用として誘導表現の表現空間を構成する．d), e) で説明することは，一般論としては非常に重要であるが，本書では§8.5以降で用いることはないので，読むのをあとまわしにしてもよい．

均衡写像　R を環，M を右 R 加群，N を左 R 加群とする．P を任意の加群とするとき，直積集合 $M\times N$ から P への写像

$$f:\ M\times N\ni(m,n)\longmapsto f(m,n)\in P$$

は，つぎの条件を満たすとき，$M\times N$ から P への**均衡写像**とよばれる：

(α)　$f(m_1+m_2,n)=f(m_1,n)+f(m_2,n)$　　$(m_1,m_2\in M,\ \ n\in N)$,

(β)　$f(m,n_1+n_2)=f(m,n_1)+f(m,n_2)$　　$(m\in M,\ \ n_1,n_2\in N)$,

(γ)　$f(mr,n)=f(m,rn)$　　$(m\in M,\ \ n\in N,\ \ r\in R)$.

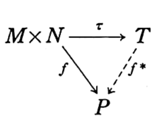
定理 8.22（テンソル積の存在と一意性）　**I（存在）**　右 R 加群 M, 左 R 加群 N に対して，つぎの性質を満たす加群 T と $M\times N$ から T への均衡写像 τ が存在する：

（i）　T の各元は，$\sum_i\tau(m_i,n_i)$（有限和）$(m_i\in M,\ n_i\in N)$ の形に書ける．

（ii）　P を任意の加群，f を $M\times N$ から P への任意の均衡写像とするとき，T から P への準同型 f^* が存在して

$$f(m,n)=f^*(\tau(m,n))\qquad(m\in M,\ \ n\in N)$$

である．



II（一意性）　(T,τ), (T',τ') がともに上の (i), (ii) を満たすとき，T から T' の上への同型 λ が存在して

$$\tau'(m,n)=\lambda(\tau(m,n))$$

である．

定義　右 R 加群 M, 左 R 加群 N に対して，定理 8.22 の (i), (ii) を満たす加

群 T と均衡写像 τ の組を，M, N の**テンソル積**といい，

$$T = M\otimes_R N, \qquad \tau(m, n) = m\otimes n$$

と書く．定理 8.22 の II により，このような T, τ は本質的に一意的である．

定理 8.22 の証明 直積集合 $M\times N$ の元を基底とする（整数環 $\boldsymbol{Z}$ 上の）自由加群を F とする．F は整数を係数とする形式的有限和

$$\sum_{i,j} z_{ij}(m_i, n_j) \qquad (z_{ij}\in \boldsymbol{Z},\ \ (m_i, n_j)\in M\times N)$$

からなる集合で，和は自然に

$$\sum_{i,j} z_{ij}(m_i, n_j)+\sum_{i,j} z_{ij}'(m_i, n_j) = \sum_{i,j} (z_{ij}+z_{ij}')(m_i, n_j)$$

と定義するのである．

さて，H をつぎのような元で生成される F の部分加群としよう：

$$(*)\qquad \begin{aligned} &(m_1+m_2, n)-(m_1, n)-(m_2, n), \\ &(m, n_1+n_2)-(m, n_1)-(m, n_2), \end{aligned} \qquad (m_i, m\in M,\ \ n_i, n\in N),$$
$$(m, rn)-(mr, n) \qquad (m\in M,\ \ n\in N,\ \ r\in R).$$

F の H による剰余群を T，F から T への自然準同型を τ としよう：

$$T = F/H, \qquad \tau(m, n) = (m, n)+H.$$

以下，(T, τ) が定理の条件 (i), (ii) を満たすことを示そう．まず，$(*)$ の形の元が H に含まれていることから，

$$(**)\qquad \begin{aligned} \tau(m_1+m_2, n) &= \tau(m_1, n)+\tau(m_2, n), \\ \tau(m, n_1+n_2) &= \tau(m, n_1)+\tau(m, n_2), \\ \tau(mr, n) &= \tau(m, rn) \end{aligned}$$

がわかる．すなわち τ は $M\times N$ から T への均衡写像である．$F\ni x=\sum_{i,j} z_{ij}(m_i, n_j)$ のとき，

$$x+H = \sum_{i,j} z_{ij}\tau(m_i, n_j)$$

であるが，$(**)$ の最初の二つの式から，

$$z_{ij}\tau(m_i, n_j) = \tau(z_{ij}m_i, n_j) = \tau(m_i, z_{ij}n_j)$$

であるから，T の各元は，$\tau(m, n)$ $(m\in M,\ n\in N)$ なる形の元の有限和であることがわかる．すなわち (T, τ) は定理の (i) を満たす．つぎに f を $M\times N$ から加群 P への均衡写像としよう．F は，(m, n) $(m\in M,\ n\in N)$ を基底とする自由加

群であるから，補題3.3[1] (p. 81) の (i) により

$$f'((m,n)) = f(m,n)$$

なる F から P への準同型 f' が存在する．このとき，f が均衡写像であることから，$H \subseteqq \mathrm{Ker}\, f'$ であるから，f' は $T=F/H$ から P への準同型 f^* で

$$f^*((m,n)+H) = f'((m,n)) = f(m,n)$$

なるものを誘導する (問1.27)．これは，

$$f^*(\tau(m,n)) = f(m,n)$$

すなわち (T,τ) が定理の (ii) を満たすことを示す．最後に (T,τ), (T',τ') がともに (i), (ii) を満たすとしよう．(ii) における P, f として T', τ' をとれば，T から T' への準同型 λ で

$$\lambda(\tau(m,n)) = \tau'(m,n)$$

を満たすものが存在する．同様に (T',τ') が (ii) を満たすことから，

$$\mu(\tau'(m,n)) = \tau(m,n)$$

を満たす T' から T への準同型 μ が存在する．T, T' はそれぞれ $\tau(m,n), \tau'(m,n)$ で生成されるから，$\mu\lambda, \lambda\mu$ はそれぞれ T, T' の恒等写像となり，とくに λ は T から T' の上への同型写像である．▌

テンソル積 $(M\otimes_R N, m\otimes n)$ の要点を再録すると，

(8.46)　加群 $M\otimes_R N$ の各元は $m\otimes n$ の形の元の有限和として表わされる．

(8.47)　$$\begin{aligned} &(m_1+m_2)\otimes n = m_1\otimes n + m_2\otimes n, \\ &m\otimes(n_1+n_2) = m\otimes n_1 + m\otimes n_2, \end{aligned} \qquad (m_i, m \in M,\ \ n_i, n \in N),$$
$$mr\otimes n = m\otimes rn \qquad (m\in M,\ \ n\in N,\ \ r\in R).$$

(8.48)　$M\times N$ から任意の加群 P への任意の均衡写像 f に対して

$$\lambda(m\otimes n) = f(m,n)$$

なる $M\otimes_R N$ から P への準同型 λ が存在する．

補題 8.8　(i)　M, M' を右 R 加群，N, N' を左 R 加群，f を M から M' への R 準同型，g を N から N' への R 準同型とする．このとき，$M\otimes_R N$ から $M'\otimes_R N'$ への準同型 $f\otimes g$ で

$$(f\otimes g)(m\otimes n) = f(m)\otimes g(n)$$

---

1)　補題3.3は階数が無限の自由加群に対しても成り立つ．

なるものがただ一つ存在する.

(ii) さらに M'' を右 R 加群, N'' を左 R 加群, f' を M' から M'' への R 準同型, g' を N' から N'' への R 準同型とするとき,

$$(f'\otimes g')(f\otimes g) = f'f\otimes g'g$$

である.

証明 (i) $(m, n)\mapsto f(m)\otimes g(n)$ は均衡写像であるから, 定理 8.22 の (ii) が適用できる. 詳しくは読者自ら確かめよ. (ii) は (i) から明らかである. ▌

補題 8.9 M を右 R 加群, N を左 R 加群とする.

$$M = M_1\oplus M_2 \qquad (\text{右 } R \text{ 加群の直和分解})$$

ならば,

$$M\otimes_R N \simeq M_1\otimes_R N\oplus M_2\otimes_R N \tag{8.49}$$

である.

証明 $\varepsilon_1, \varepsilon_2$ をそれぞれ M から M_1, M_2 への射影とする. $\varepsilon_1, \varepsilon_2$ は R 準同型で

$$\varepsilon_1+\varepsilon_2 = 1, \quad {\varepsilon_1}^2 = \varepsilon_1, \quad {\varepsilon_2}^2 = \varepsilon_2, \quad \varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1 = 0,$$

$$\varepsilon_1(m_1) = m_1 \quad (m_1\in M_1), \qquad \varepsilon_2(m_2) = m_2 \quad (m_2\in M_2)$$

である. $\theta_i=\varepsilon_i\otimes 1$ (補題 8.8 の (i) 参照, 1 は N の恒等写像) とおくと, 補題 8.8 により

$$1 = \theta_1+\theta_2, \quad {\theta_1}^2 = \theta_1, \quad {\theta_2}^2 = \theta_2, \quad \theta_1\theta_2 = \theta_2\theta_1 = 0$$

である. よって

$$T_i = \theta_i(M\otimes_R N)$$

とおくと,

$$M\otimes_R N = T_1\oplus T_2$$

なる直和分解が得られる. (8.49) を証明するために

$$T_i \simeq M_i\otimes_R N \qquad (i=1, 2)$$

を示そう. $M_1\times N\ni(m_1, n)$ とすると

$$m_1\otimes n = \varepsilon_1(m_1)\otimes n = (\varepsilon_1\otimes 1)(m_1\otimes n) = \theta_1(m_1\otimes n)$$

であるから $m_1\otimes n\in T_1$ である. よって $M_1\times N$ から T_1 への写像 $(m_1, n)\mapsto m_1\otimes n$ を考えると, これは均衡写像である. また $m=m_1+m_2$ $(m_i\in M_i)$ のとき, $\theta_1(m\otimes n)=\theta_1(m_1\otimes n)=m_1\otimes n$ であるから, T_1 は $m_1\otimes n$ $(m_1\in M_1,\ n\in N)$ で生成される. P を加群として, g を $M_1\times N$ から P への均衡写像としよう.

$$\begin{array}{ccccc} M\times N & \xrightarrow{\varepsilon_1\times 1} & M_1\times N & \xrightarrow{g} & P \\ & \searrow^{\otimes} & & \nearrow_{g^*} & \\ & & M\otimes_R N & & \end{array}$$

上の図式を考えると，$M\otimes_R N$ から P への準同型 g^* が存在する．g^* の T_1 への制限を g_1 とすると，

$$\begin{aligned} g_1(m_1\otimes n) &= g^*(m_1\otimes n) \\ &= g\circ(\varepsilon_1\times 1)(m_1, n) \\ &= g(\varepsilon_1(m_1), n) \\ &= g(m_1, n) \qquad (m_1\in M_1,\ n\in N) \end{aligned}$$

であるから，$(T_1, m_1\otimes n)$ は定理8.22の(i), (ii)を満たす．したがって，$T_1\simeq M_1\otimes_R N$ である．▌

注意　補題8.9は，$M=M_1\oplus M_2$ のとき，$M_1\otimes_R N$ を $M\otimes_R N$ の部分加群とみなせることを示している．より詳しく，補題8.9の証明から，$M_1\otimes_R N$ を $m_1\otimes n$ $(m_1\in M_1,\ n\in N)$ なる $M\otimes_R N$ の元で生成される部分加群と同一視することができることが分る．しかし，一般には M_1 が M の部分加群のとき，$M_1\otimes_R N$ を $M\otimes_R N$ の部分加群とみなすことはできない．たとえば，容易に分るように $N=\boldsymbol{Z}/2\boldsymbol{Z}$ のとき，$\boldsymbol{Q}\otimes_{\boldsymbol{Z}}N=0$ ($\boldsymbol{Q}$ は有理数の加法群)，$\boldsymbol{Z}\otimes_{\boldsymbol{Z}}N\simeq N$ である．

問 8.20　R を環，N を左 R 加群とするとき，$R\otimes_R N\simeq N$ を示せ．同様に右 R 加群 M に対して $M\otimes_R R\simeq M$ である．——

テンソル積 $M\otimes_R N$ は，一般には作用環をもたない単なる加群である．しかし，しばしば $M\otimes_R N$ を或る環の上の(右または左)加群とみなせる場合が起こる．S, R を環としよう．加群 V が (S, R) **加群**とは，

(α)　V は左 S 加群かつ右 R 加群,

(β)　$(sv)r = s(vr)$　$(s\in S,\ v\in V,\ r\in R)$

が成り立つことである．環 R は自然に (R, R) 加群である．また R が可換環ならば，任意の左 R 加群 V は

$$vr = rv \qquad (v\in V,\ r\in R)$$

とおくことにより右 R 加群とみなせる．同様に可換環上の右加群は左加群とみなせる．よって可換環 R 上の(右または左)加群は，つねに (R, R) 加群である．

さて，M が (S, R) 加群であるとき，$M\otimes_R N$ をつぎのようにして左 S 加群と

みることができる:

$$s(m\otimes n) = sm\otimes n \qquad (s\in S,\ m\in M,\ n\in N).$$

実際，$S\ni s$ のとき，$M\times N$ から $M\otimes_R N$ への写像

$$(m, n)\longmapsto sm\otimes n$$

は均衡写像であるから，$M\otimes_R N$ の自己準同型 φ_s で

$$\varphi_s(m\otimes n) = sm\otimes n$$

なるものが存在する．このとき

$$sv = \varphi_s(v) \qquad (v\in M\otimes_R N)$$

とおくと，$M\otimes_R N$ が左 S 加群の公理を満たすことは容易にわかる．このように $M\otimes_R N$ を左 S 加群とみるとき，

$$s(\sum m_i\otimes n_i) = \sum sm_i\otimes n_i$$

が成り立つ．

問 8.21 問 8.20 における同型 $R\otimes_R N\simeq N$ は左 R 加群としての同型であることを確かめよ．同様に $M\otimes_R R\simeq M$ は右 R 加群としての同型である．——

補題 8.9 において $M=M_1\oplus M_2$ が (S, R) 加群としての直和分解ならば，$M\otimes_R N\simeq M_1\otimes_R N\oplus M_2\otimes_R N$ は左 S 加群としての直和分解である．また補題 8.8 においても，M, M' が (S, R) 加群で f が M から M' への (S, R) 準同型すなわち

$$f(svr) = sf(v)r \qquad (s\in S,\ v\in V,\ r\in R)$$

が成り立つならば，$f\otimes g$ は左 S 加群 $M\otimes_R N$ から $M'\otimes_R N$ への S 準同型である．これらのことは，読者自ら確かめられたい．

例 8.16 線型空間のテンソル積 V, U を体 k 上の線型空間とする．V を (k, k) 加群とみるとき，$V\otimes_k U$ は左 k 加群すなわち k 上の線型空間である．V の k 上の次元を r とすると

$$V\simeq \underbrace{k\oplus k\oplus\cdots\oplus k}_{r} \qquad (k \text{ 加群としての同型})$$

であるから，補題 8.9 により

$$V\otimes_k U\simeq \underbrace{k\otimes U\oplus\cdots\oplus k\otimes U}_{r}$$

を得る．問 8.21 により $k\otimes U\simeq U$ であるから，U の k 上の次元が s ならば，

$$\dim_k V\otimes_k U = rs$$

である．$v_1, v_2, \cdots, v_r$ を V の k 上の基底，$u_1, u_2, \cdots, u_s$ を U の k 上の基底とするとき，$V\otimes_k U$ の任意の元は，$v_i\otimes u_j$ $(1\leqq i\leqq r,\ 1\leqq j\leqq s)$ の k 上の線型結合として表わせるから，$v_i\otimes u_j$ $(1\leqq i\leqq r,\ 1\leqq j\leqq s)$ が $V\otimes_k U$ の k 上の基底となる．

補題 8.10（テンソル積の結合則） R, S を環，L を右 R 加群，M を (R, S) 加群，N を左 S 加群とするとき，

(8.50) $$(L\otimes_R M)\otimes_S N \simeq L\otimes_R (M\otimes_S N)$$

である．L が (T, R) 加群ならば，(8.50) は T 加群としての同型である．——

証明は読者自ら試みられたい．

e）誘導表現の表現空間

H を有限群 G の部分群，V を左 $k[H]$ 加群とする．$k[G]$ を自然に $(k[G], k[H])$ 加群とみるとき，テンソル積 $k[G]\otimes_{k[H]}V$ は左 $k[G]$ 加群である．これを以後簡単に V^G と書くことがある：

$$V^G = k[G]\otimes_{k[H]}V.$$

V が与える H の k 上の表現（§8.1, c)）を (ρ, V) とするとき，V^G の与える G の k 上の表現を (ρ^G, V^G) と書き，(ρ, V) の**誘導表現**という．

G の H による左剰余類分解を

$$G = x_1H+x_2H+\cdots+x_nH, \qquad n = [G:H]$$

とすると，明らかに

$$k[G] = x_1k[H]\oplus\cdots\oplus x_nk[H]$$

なる右 $k[H]$ 加群としての直和分解が得られる．よって補題 8.9 により

$$V^G = (x_1k[H]\otimes V)\oplus\cdots\oplus(x_nk[H]\otimes V),$$
$$x_ik[H]\otimes V = \langle x_iy\otimes v \mid y\in k[H],\ v\in V\rangle$$

なる（k 加群としての）直和分解が得られる．ところで

$$x_iy\otimes v = x_i\otimes yv \qquad (y\in k[H],\ v\in V)$$

であるから，

$$x_ik[H]\otimes V = x_i\otimes V = \{x_i\otimes v\in V^G \mid v\in V\}$$

と書くことができる．よって

(8.51) $$V^G = (x_1\otimes V)\oplus\cdots\oplus(x_n\otimes V)$$

なる k 加群としての直和分解が得られる．一方，明らかに

$$x_ik[H]\simeq k[H] \qquad (\text{右 } k[H] \text{ 加群としての同型})$$

であるから，問 8.21 を用いて

$$x_i k[H]\otimes_{k[H]} V \simeq k[H]\otimes_{k[H]} V \simeq V \qquad (k \text{ 同型}).$$

よって

$$V^G \simeq \underbrace{V\oplus\cdots\oplus V}_{n} \qquad (k \text{ 同型})$$

を得る．これから

$$\dim_k V^G = n\dim_k V = [G:H]\dim_k V$$

を得る．とくに，$v_1, v_2, \cdots, v_m$ を V の k 上の基底とするとき，(8.51) により

$$x_i\otimes v_j \qquad (1\leqq i\leqq n,\ 1\leqq j\leqq m)$$

は，V^G の k 上の基底である．さて，左 $k[H]$ 加群 V から得られる H の表現 (ρ, V) の基底 $v_1, v_2, \cdots, v_m$ に関する行列表示を

$$R(h) = (r_{ij}(h)) \qquad (h\in H)$$

とするとき，(ρ^G, V^G) の基底 $x_i\otimes v_j$ に関する行列表示が，a) で与えられた $R^G(x)\,(x\in G)$ と一致することを示そう．$G\ni x$ に対して

$$xx_i = x_k h \qquad (h\in H)$$

とするとき，

$$\begin{aligned} x(x_i\otimes v_j) &= xx_i\otimes v_j = x_k h\otimes v_j = x_k\otimes hv_j \\ &= x_k\otimes\sum_{s=1}^{m} r_{sj}(h)v_s \\ &= \sum_{s=1}^{m} r_{sj}(h)x_k\otimes v_s \end{aligned}$$

である．$k(H)$ の元 $r_{sj}(h)$ を

$$\alpha_{sj}(x) = \begin{cases} r_{sj}(x) & (x\in H), \\ 0 & (x\notin H) \end{cases}$$

によって $k(G)$ の元に拡張すれば，上の式は

$$x(x_i\otimes v_j) = \sum_{s=1}^{m}\sum_{k=1}^{n}\alpha_{sj}(x_k{}^{-1}xx_i)(x_k\otimes v_s)$$

となる．これは，V^G の基底 $x_i\otimes v_j$ を

$$x_1\otimes v_1, \quad \cdots, \quad x_1\otimes v_m, \quad \cdots, \quad x_n\otimes v_1, \quad \cdots, \quad x_n\otimes v_m$$

と並べると，この基底に関して (ρ^G, V^G) に対応する行列が

$$R^G(x) = (R^0(x_i{}^{-1}xx_j)),$$

$$R^0(x_i^{-1}xx_j) = \begin{cases} R(x_i^{-1}xx_j) & (x_i^{-1}xx_j \in H), \\ 0 & (x_i^{-1}xx_j \notin H) \end{cases}$$

であることを示す.

V_1, V_2 を $k[H]$ 加群とするとき, 補題 8.9 により

$$(V_1 \oplus V_2)^G \simeq V_1^G \oplus V_2^G$$

が成り立つ. これから, k を複素数体, φ_1, φ_2 をそれぞれ $\boldsymbol{C}[H]$ 加群 V_1, V_2 から得られる H の $\boldsymbol{C}$ 上の表現の指標とするとき,

$$(\varphi_1+\varphi_2)^G = \varphi_1^G + \varphi_2^G$$

となる. これが, §8.4, b) の最後で述べた (8.42) である. また V を $k[H]$ 加群, K を $K \supseteq H$ なる G の部分群とするとき, 補題 8.10 により

$$(V^K)^G \simeq V^G$$

が成り立つ. 上と同様にして, 指標を考えれば (8.43) が得られる.

問 8.22 U を左 $k[G]$ 加群, H を G の部分群とする. V をつぎの性質をもつ U の部分空間とする:

(i) V は $k[H]$ 不変すなわち $yV \subseteq V$ $(\forall y \in k[H])$,

(ii) G の或る左剰余類分解 $G = x_1H + x_2H + \cdots + x_nH$ に対して

$$U = x_1V \oplus x_2V \oplus \cdots \oplus x_nV \qquad (k \text{ 加群としての直和}).$$

このとき, $V^G \ni \sum_i x_i \otimes v \mapsto \sum_i x_i v \in U$ なる対応によって $V^G \simeq U$ ($k[G]$ 同型) であることを示せ. ——

以後, 左 $k[G]$ 加群 U と G の部分群 H に対して, U を左 $k[H]$ 加群と考えたときそれを U_H と書く. さて, H, K を G の部分群, V を左 $k[H]$ 加群とするとき, 誘導加群 V^G を部分群 K に制限した $(V^G)_K$ の $k[K]$ 加群への直和分解を与える一つの結果を示そう. この分解は **Mackey 分解**とよばれ, 表現論においてしばしば応用されるものである. まず, V^G の部分空間 $x \otimes V$ $(x \in G)$ は自然に $k[xHx^{-1}]$ 加群とみることができることに注意する. 実際,

$$(xhx^{-1})(x \otimes v) = xh \otimes v = x \otimes hv \in x \otimes V \qquad (h \in H,\ v \in V)$$

であるから, $x \otimes V$ は $k[xHx^{-1}]$ 不変である.

定理 8.23 (Mackey) K, H を G の部分群,

$$G = Kx_1H + \cdots + Kx_rH$$

を G の K, H による両側分解とする. V を左 $k[H]$ 加群とするとき,

(8.52) $$(V^G)_K \simeq \oplus \sum_{i=1}^{r} ((x_i \otimes V)_{\tilde{H}_i})^K, \quad \tilde{H}_i = x_i H x_i^{-1} \cap K$$

なる $k[K]$ 加群としての同型が成り立つ．さらに $k[K]$ 加群 $(x_i \otimes V)_{\tilde{H}_i}{}^K$ は，両側剰余類 Kx_iH によって（$k[K]$ 同型を無視して）定まり，その代表系 $x_1, x_2, \cdots, x_r$ のとり方によらない．

証明 $Kx_iH = \sum_j x_{ij}H$ を Kx_iH に含まれる H の左剰余類への分解とするとき，

$$V_i = \oplus \sum_j x_{ij} \otimes V$$

とおく．V_i は両側剰余類 Kx_iH によって定まり，分解 $\sum_j x_{ij}H$ の代表系 $\{x_{ij}\}$ のとり方によらない．実際，

$$Kx_iH = \sum_j x_{ij}H = \sum_j x_{ij}'H, \quad x_{ij} = x_{ij}'h_j \quad (h_j \in H)$$

とするとき，

$$\sum_j x_{ij} \otimes V = \sum_j x_{ij}'h_j \otimes V = \sum_j x_{ij}' \otimes h_j V = \sum_j x_{ij}' \otimes V$$

である．明らかに V_i は $k[K]$ 不変であるから，(8.51) により

$$V^G = V_1 \oplus \cdots \oplus V_r$$

なる $k[K]$ 加群としての直和分解が成り立つ．よって，以下

$$V_i \simeq (x_i \otimes V)_{\tilde{H}_i}{}^K, \quad \tilde{H}_i = x_i H x_i^{-1} \cap K$$

であることを示そう．ところで K の $\tilde{H}_i = x_i H x_i^{-1} \cap K$ による左剰余類分解を

$$K = t_1\tilde{H}_i + t_2\tilde{H}_i + \cdots + t_s\tilde{H}_i$$

とすると，

$$Kx_iH = t_1x_iH + \cdots + t_sx_iH$$

であるから，

$$V_i = \sum_{j=1}^{s} t_j x_i \otimes V = \sum_{j=1}^{s} t_j(x_i \otimes V) \qquad (k \text{ 加群としての直和}).$$

ここで右辺の $x_i \otimes V$ は $k[\tilde{H}_i]$ 加群であるから，問 8.22 により $V_i \simeq (x_i \otimes V)_{\tilde{H}_i}{}^K$ なる $k[K]$ 加群としての同型を得る．▌

$\varphi \in Cl(H)$，$x \in G$ に対して，

$$\varphi^x(y) = \varphi(xyx^{-1})$$

とおくと，$\varphi^x \in Cl(H^x)$ $(H^x = x^{-1}Hx)$ である．φ を $\boldsymbol{C}[H]$ 加群 V の指標とするとき，(8.52) から

$$\varphi^G \mid K = \sum_{i=1}^{r} (\varphi^{x_i^{-1}} \mid \tilde{H}_i)^K \tag{8.53}$$

を得る．この式の特別の場合はいままでにも現われている．すなわち例8.8における (8.31) や§8.4, b) の最後にあげた (8.45) がそれである．なお (8.53) は任意の $\varphi \in Cl(H)$ に対して成り立ち，(8.41) を用いて直接計算することによっても確かめることができる．

§8.5 ユニタリ表現

ここでは，有限群の複素数体上の任意の表現は，ユニタリ表現と同型であるという定理8.24とその一つの応用——Frobenius-Schur の定理8.25——を述べる．本節の内容は，本質的には Schur の補題の応用であるから，§8.3から続けられるべきものである．なお，Frobenius-Schur の定理8.25は，後に§8.8, a) で用いられるであろう．

定理 8.24 (ρ, V) を G の複素数体 $\boldsymbol{C}$ 上の任意の表現とするとき，V 上の正値 Hermite 形式 $f(u, v)$ が存在して

$$f(\rho(x)u, \rho(x)v) = f(u, v) \qquad (u, v \in V,\ \ x \in G) \tag{8.54}$$

が成り立つ．同様に，(ρ, V) を G の実数体 $\boldsymbol{R}$ 上の任意の表現とするとき，V 上の正値対称形式 $f(u, v)$ が存在して

$$f(\rho(x)u, \rho(x)v) = f(u, v) \qquad (u, v \in V,\ \ x \in G)$$

が成り立つ．——

まず，正値 Hermite 形式について簡単に復習しよう．V を複素数体 $\boldsymbol{C}$ 上の線型空間とするとき，$V \times V$ から $\boldsymbol{C}$ への写像

$$V \times V \ni (u, v) \longmapsto f(u, v) \in \boldsymbol{C}$$

は，

(α) $f(u, v) = \overline{f(v, u)}$ (　は複素共役を表わす),

(β) $f(u+u', v) = f(u, v) + f(u', v)$,

(γ) $f(\alpha u, v) = \alpha f(u, v)$

を満たすとき，**Hermite 形式**とよばれる．さらに

(δ) $f(u, u) > 0 \quad (V \ni \forall u \neq 0)$

が成り立つとき，$f(u, v)$ を**正値 Hermite 形式**あるいは**内積**という．$f(u, v)$ が n 次元線型空間の上の内積であるとき，いわゆる Schmidt の直交化の方法によって

$$f(u_i, u_j) = \delta_{ij} \qquad (\delta_{ij} \text{ は Kronecker のデルタ})$$

を満たす V の基底 $u_1, u_2, \cdots, u_n$ が存在する．このような基底を V の**正規直交基底**という．V の線型変換 ρ が

$$(8.55) \qquad f(u, v) = f(\rho(u), \rho(v)) \qquad (u, v \in V)$$

を満たすとき，正規直交基底に関して ρ に対応する行列はユニタリ行列である．V を $\boldsymbol{C}$ 上の任意の n 次元線型空間とするとき，V 上に内積が存在する．実際，V の任意の基底 $u_1, u_2, \cdots, u_n$ をとり，$u = \sum_{i=1}^{n} \alpha_i u_i$，$v = \sum_{i=1}^{n} \beta_i u_i$ $(\alpha_i, \beta_i \in \boldsymbol{C})$ に対して

$$f(u, v) = \sum_{i=1}^{n} \alpha_i \bar{\beta}_i$$

とおくと，$f(u, v)$ は V の内積である．実数体 $\boldsymbol{R}$ 上の線型空間に対して，まったく平行に**対称形式**，**正値対称形式**(これも内積とよぶことがある)の概念が定義される．上の (α) は，

$(\alpha)'$ $f(u, v) = f(v, u) \in \boldsymbol{R}$

と簡単になることに注意．正値対称形式に対して，(8.55) を満たす変換 ρ は，正規直交基底に関して実直交行列で表わされる．

定理 8.24 の証明 $f(u, v)$ を V 上の任意の内積とする．このとき，

$$f^*(u, v) = \sum_{x \in G} f(\rho(x)u, \rho(x)v)$$

とおくと，$f^*(u, v)$ も V 上の内積であることは容易に確かめられる．また，

$$\begin{aligned} f^*(\rho(x)u, \rho(x)v) &= \sum_{y \in G} f(\rho(y)\rho(x)u, \rho(y)\rho(x)v) \\ &= \sum_{y \in G} f(\rho(yx)u, \rho(yx)v) \\ &= \sum_{y \in G} f(\rho(y)u, \rho(y)v) \\ &= f^*(u, v) \end{aligned}$$

となり，$f^*(u, v)$ は (8.54) を満たす．▌

定理 8.24 を用いて，複素数体(あるいは実数体)上の表現 (ρ, V) の完全可約性 (Maschke の定理 8.1) を証明することができる．実際，(ρ, V) を有限群 G の $\boldsymbol{C}$ 上の表現，U を V の ρ 不変部分空間とする．$f(u, v)$ を (8.54) を満たす V 上の内積とするとき，U の直交補空間

$$U^{\perp} = \{v \in V \mid f(v, u) = 0 \ (\forall u \in U)\}$$

は，ρ 不変であることが容易にわかる．$V = U \oplus U^{\perp}$ であるから，定理 8.1 の証明における命題(＊)が成り立つ．

(ρ, V) を G の $\boldsymbol{C}$ 上の表現，χ をその指標とする．$\chi = \bar{\chi}$ で，(ρ, V) が G の実数体 $\boldsymbol{R}$ 上の表現と($\boldsymbol{C}$ で)同型のとき，(ρ, V) を**第1種**，(ρ, V) が G の $\boldsymbol{R}$ 上の表現と同型でないとき**第2種の表現**という．$\chi \neq \bar{\chi}$ のとき (ρ, V) を**第3種の表現**という．第1種表現は，適当な行列表示が実数を成分とする行列であるものにほかならない．第2種表現は，指標の値は実数であるが，どのような行列表示をとっても行列の成分を実数にすることができないものである．指標が実数値でないものが，第3種表現である．G の行列表現 $x \mapsto R(x)$ $(\forall x \in G)$ が，すべての x に対して $R(x)$ がユニタリ行列であるとき，**ユニタリ表現**ということにしよう．定理 8.24 は，G の $\boldsymbol{C}$ 上の任意の表現の適当な行列表示がユニタリ表現になることを主張している．

補題 8.11　(i)　$R_1(x)$, $R_2(x)$ を G の既約ユニタリ表現とする．$R_1(x)$ と $R_2(x)$ が同値すなわち $R_1(x)S = SR_2(x)$ $(\forall x \in G)$ を満たす正則行列 S が存在するならば，このような S としてユニタリ行列をとることができる．

(ii)　$R(x)$ を既約ユニタリ表現，U を

$$U^{-1}R(x)U = \overline{R(x)} \qquad (\forall x \in G)$$

なるユニタリ行列とする(したがって $R(x)$ は第1種または第2種の表現である)．このとき，

$${}^tU = U \quad \text{または} \quad {}^tU = -U$$

である．さらに ${}^tU = U$ であるためには，$R(x)$ が G の第1種表現であることが必要十分である．

証明　$R(x)$ を G の既約行列表現とするとき，

(＊)　$S^{-1}R(x)S = T^{-1}R(x)T \quad (\forall x \in G) \Longrightarrow ST^{-1} =$ スカラー行列

である．これは Schur の補題 8.1 の (ii) の直接の結果である．さて (i) における $R_1(x), R_2(x), S$ に対して，$S^{-1}R_1(x)S = R_2(x)$ より $S^*R_1(x)^*(S^*)^{-1} = R_2(x)^*$，$R_1(x)$, $R_2(x)$ はユニタリ行列であるから，$S^*R_1(x)^{-1}(S^*)^{-1} = R_2(x)^{-1}$．したがって $S^*R_1(x)(S^*)^{-1} = R_2(x) = S^{-1}R_1(x)S$ $(\forall x \in G)$ である．よって(＊)により $SS^* = \alpha E$ ($\alpha \in \boldsymbol{C}$, E は単位行列)．このとき，明らかに $\alpha > 0$ であるから，$\alpha = \beta\bar{\beta}$

なる $\beta \in \boldsymbol{C}$ をとり，$U=(1/\beta)S$ とおくと，U はユニタリ行列で，$U^{-1}R_1(x)U=R_2(x)$ となる．よって (i) が証明された．

(ii) $U^{-1}R(x)U=\overline{R(x)}$ より $\bar{U}^{-1}\overline{R(x)}\bar{U}=R(x)$．よって $(U\bar{U})^{-1}R(x)U\bar{U}=R(x)$．($*$) により，$U\bar{U}=\alpha E$ である．U はユニタリ行列であるから $\bar{U}={}^tU^{-1}$．よって $U=\alpha{}^tU$．この両辺の転置行列をとれば ${}^tU=\alpha U=\alpha^2\cdot{}^tU$．よって $\alpha=\pm 1$ である．$R(x)$ が第1種の表現すなわち $S^{-1}R(x)S$ がすべての x に対して実行列であるような正則行列 S が存在したとしよう．このとき，$\bar{S}^{-1}\overline{R(x)}\bar{S}=S^{-1}R(x)S$ および $U^{-1}R(x)U=\overline{R(x)}$ より $(U\bar{S}S^{-1})^{-1}R(x)(U\bar{S}S^{-1})=R(x)$．よって ($*$) により $U\bar{S}S^{-1}=\alpha E$ なる $\alpha \in \boldsymbol{C}$ が存在する．このとき，$U=\alpha S\bar{S}^{-1}$ より，${}^tU=\bar{U}^{-1}=(\overline{\alpha S\bar{S}^{-1}})^{-1}=\bar{\alpha}^{-1}S\bar{S}^{-1}$ であるから，${}^tU=-U$ ならば $\bar{\alpha}^{-1}S\bar{S}^{-1}=-\alpha S\bar{S}^{-1}$，よって $\alpha\bar{\alpha}=-1$ となり矛盾である．すなわち $R(x)$ が第1種ならば，${}^tU=U$ である．逆に ${}^tU=U$ としよう．このとき，

$$(**) \qquad V^2=U, \quad {}^tV=V$$

なるユニタリ行列 V が存在する．実際，$T^{-1}UT=D$ が対角行列になるようにユニタリ行列 T をとれば，${}^tU=U$ より ${}^tTTD=D{}^tTT$ である．このとき ${}^tTT$ と D を同時に対角化することにより ${}^tTTE=E{}^tTT$，$E^2=D$ なる対角行列 E の存在がわかる．このとき，$TET^{-1}=V$ とおけばよい．($**$) より

$$\begin{aligned}\overline{V^{-1}R(x)V} &= \bar{V}^{-1}\overline{R(x)}\bar{V} = V(U^{-1}R(x)U)V^{-1}\\ &= V(V^{-2}R(x)V^2)V^{-1} = V^{-1}R(x)V\end{aligned}$$

となり，$R(x)$ は第1種である．▌

定理 8.25 (Frobenius-Schur)　χ を G の既約指標とする．

$$\nu(\chi)=\frac{1}{|G|}\sum_{x\in G}\chi(x^2)$$

とおくと

$$\nu(\chi)=\begin{cases} 1 & (\chi\,(\text{に対応する表現})\text{ が第1種のとき}),\\ -1 & (\chi\text{ が第2種のとき}),\\ 0 & (\chi\text{ が第3種のとき}).\end{cases}$$

証明　$R(x)$ $(x\in G)$ を指標 χ をもつユニタリ表現とする．$R(x)=(r_{ij}(x))$ とすると，

$$(*)\qquad \nu(\chi)=\frac{1}{|G|}\sum_{x\in G}\chi(x^2)=\frac{1}{|G|}\sum_{x\in G}\mathrm{tr}\,(R(x^2))$$
$$=\frac{1}{|G|}\sum_{x\in G}\mathrm{tr}\,(R(x)R(x))=\frac{1}{|G|}\sum_{x\in G}\mathrm{tr}\,(R(x)\,\overline{{}^tR(x^{-1})})$$
$$=\frac{1}{|G|}\sum_{x\in G}\sum_{i,j}r_{ij}(x)\overline{r_{ij}(x^{-1})}$$
$$=\sum_{i,j}\langle r_{ij},\bar{r}_{ij}\rangle\qquad(\S 8.2,\ \mathrm{c}),\ (8.18)).$$

$\chi\neq\bar{\chi}$ ならば $R(x)$ と $\overline{R(x)}$ は同値でないから，Schur の関係式 (8.19) により $\langle r_{ij},\bar{r}_{ij}\rangle=0$. よって $\nu(\chi)=0$ を得る．χ が第1種ならば，定理 8.8 により $R(x)$ は実直交行列としてよいから，Schur の関係式 (8.20) より

$$\langle r_{ij},r_{ij}\rangle=\frac{1}{\deg\chi}\delta_{ij}.$$

よって

$$\nu(\chi)=\sum_{i,j}\frac{1}{\deg\chi}\delta_{ij}=1$$

を得る．最後に χ は第2種であるとしよう．補題 8.11 により，

$$U^{-1}R(x)U=\overline{R(x)},\qquad {}^tU=-U$$

なるユニタリ行列 U が存在する．$U=(u_{ij})$ とするとき，

$$\overline{R(x^{-1})}=U^{-1}R(x^{-1})U=-\bar{U}R(x^{-1})U$$

であるから

$$\overline{r_{ij}(x^{-1})}=-\sum_{s,t}\bar{u}_{is}r_{st}(x^{-1})u_{tj}$$

である．これを $(*)$ の最後の式に代入すると，

$$\nu(\chi)=-\sum_{i,j}\sum_{s,t}\langle r_{ij},r_{st}\rangle\bar{u}_{is}u_{tj}$$
$$=-\sum_{i,j}\sum_{s,t}\frac{\delta_{it}\delta_{js}}{\deg\chi}\bar{u}_{is}u_{tj}\qquad((8.20)\ による)$$
$$=-\frac{1}{\deg\chi}\sum_{i,j}\bar{u}_{ij}u_{ij}$$
$$=-1$$

を得る．▌

例 8.17 位数8の正2面体群 D_8 の2次既約指標を χ としよう（例 8.10 参照）．

$$D_8=\langle a,b\mid b^2=a^4=1,\ b^{-1}ab=a^{-1}\rangle$$

とするとき，

$$\chi(a^ib)=0 \quad (0\leqq i\leqq 3), \qquad \chi(a)=\chi(a^3)=0, \qquad \chi(a^2)=-2$$

である．したがって

$$\nu(\chi)=\frac{1}{8}\left(\chi(1)+\chi(a^2)+\chi(a^4)+\chi(a^6)+\sum_{i=0}^{3}\chi((a^ib)^2)\right)$$
$$=\frac{1}{8}(2-2+2-2+4\times 2)=1$$

である．すなわち χ に対応する表現は実行列で表わされ，実際

$$a\longmapsto\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \qquad b\longmapsto\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

なる表現の指標が χ である．Q_8 を位数 8 の 4 元数群としよう：

$$Q_8=\langle a, b\mid a^4=1,\ a^2=b^2,\ b^{-1}ab=a^{-1}\rangle.$$

Q_8 は，

$$\chi(1)=2, \quad \chi(a^2)=-2, \quad \chi(a)=\chi(a^3)=0, \quad \chi(a^ib)=0 \quad (0\leqq i\leqq 3)$$

なる 2 次の既約指標をもつ（問 8.10 参照）．このとき，

$$\nu(\chi)=\frac{1}{8}(2-2+2-2+4\times(-2))=-1$$

となり，χ に対応する表現は，指標 χ の値が整数（とくに実数）であるにもかかわらず，決して実行列では表わされない．——

Frobenius-Schur の定理 8.25 は，$\nu(\chi)$ の値によって χ に対応する表現が，実数体上の表現と同型であるかどうかを判定できることを示しているのであるが，それを除いても $\nu(\chi)=(1/|G|)\sum_{x\in G}\chi(x^2)$ の値が 0 または ±1 に限るという事実は既約指標の一つの著しい性質であるというべきである．後の §8.8 においてこの事実の応用を与えるであろう．

§8.6 Brauer の指標定理

ここでは，Brauer の指標定理 8.26 を証明する．この定理は多くの重要な応用をもつが，本書では既約指標の値についての興味ある一性質——Brauer の定理 8.29——と，J. A. Green による一つの補題をその応用例としてあげる．さらに，この J. A. Green の補題を用いて $GL(2, q)$ の既約指標を決定する．最後に Clifford の定理 8.18 を用いて，$GL(2, q)$ の既約指標から，$SL(2, q)$ の既約指標を求める．

a) Brauer の指標定理

§8.4, c) におけるように有限群 G の既約指標の全体を Irr(G) で表わす．Irr$(G)=\{\chi_1, \chi_2, \cdots, \chi_h\}$ とするとき，$\chi_1, \chi_2, \cdots, \chi_h$ の整係数1次結合

$$\sum_{i=1}^{h} a_i\chi_i \qquad (a_i \in \boldsymbol{Z})$$

を G の**一般指標**という．$a_i \geqq 0\,(i=1, 2, \cdots, h)$ のとき，$\sum_{i=1}^{h} a_i\chi_i$ は表現の指標である．一般指標の全体を $Cl_{\boldsymbol{Z}}(G)$ で表わす．$\chi_i\chi_j$ は G の指標であるから ((8.27))，$\chi_i\chi_j \in Cl_{\boldsymbol{Z}}(G)$ である．したがって $Cl_{\boldsymbol{Z}}(G)$ は可換環であることがわかる．恒等指標 1_G が $Cl_{\boldsymbol{Z}}(G)$ の乗法の単位元である．$Cl_{\boldsymbol{Z}}(G)$ を G の**指標環**という．

補題 8.12　$\theta \in Cl_{\boldsymbol{Z}}(G)$ とする．θ が既約指標であるためには，

(i)　$\theta(1) > 0$,

(ii)　$(\theta, \theta) = 1$

であることが必要十分である．

証明　必要であることは明らかである．$\theta=\sum_{i=1}^{h} a_i\chi_i\ (a_i \in \boldsymbol{Z})$ としよう．直交関係により $1=(\theta, \theta)=\sum_{i=1}^{h} a_i^2$ であるから，或る i に対して $a_i=\pm 1$, $i \neq j$ ならば $a_j=0$ となり，$\theta=\pm\chi_i$ を得るが，$\theta(1)>0$ であるから $\theta=\chi_i$ でなければならない．∎

さて，Brauer の指標定理は二つの内容をもつのであるが，それを述べる前に言葉の定義をしなければならない．

G の部分群 E は，

$$E = P \otimes C, \qquad P = \text{或る素数 } p \text{ に対する } p \text{ 群},$$
$$C = \text{位数が } p \text{ と素な巡回群}$$

なる構造をもつとき，**基本部分群**とよばれる．素数 p に言及したいときは，**p 基本部分群**という．基本部分群は巾零群であり，p 基本部分群の部分群は p 基本部分群である．

定理 8.26 (Brauer の指標定理)　(i)　G の類関数 f が一般指標であるためには，f の任意の基本部分群 E への制限 $f|E$ が，E の一般指標であることが必要十分である．

(ii)　G の任意の指標は，いくつかの基本部分群の1次指標の誘導指標の整係数1次結合で表わされる．——

この定理の証明に入る前に準備をしておこう．$\mathcal{E}_G$ によって G の基本部分群全

体の集合を表わす．また，

$$\mathcal{R}(G,\mathcal{E}_G)=\{f\in Cl(G)\mid f|E\in Cl_{\boldsymbol{Z}}(E)\ (\forall E\in\mathcal{E}_G)\},$$

$$\mathcal{I}(G,\mathcal{E}_G)=\left\{f\in Cl(G)\,\middle|\,f=\sum_i a_i\varphi_i{}^G,\ \varphi_i\in\mathrm{Irr}\,(E_i),\ E_i\in\mathcal{E}_G\right\}$$

とおく．$\mathcal{R}(G,\mathcal{E}_G)$ は G の類関数 f で，f の任意の基本部分群への制限 $f|E$ が，E の一般指標となっているもの全体の集合であり，$\mathcal{I}(G,\mathcal{E}_G)$ は，いくつかの基本部分群 $E_1,E_2,\cdots,E_s$ をとり，基本部分群 E_i の既約指標 φ_i の誘導指標 $\varphi_i{}^G$ の整係数1次結合全体の集合である．このとき，

$$\mathcal{I}(G,\mathcal{E}_G)\subseteqq Cl_{\boldsymbol{Z}}(G)\subseteqq\mathcal{R}(G,\mathcal{E}_G)\tag{8.56}$$

は明らかである．$\mathcal{R}(G,\mathcal{E}_G)$ は，

$$\begin{aligned}(f+g)(x)&=f(x)+g(x),\\(fg)(x)&=f(x)g(x)\end{aligned}\qquad(f,g\in\mathcal{R}(G,\mathcal{E}_G),\ \ x\in G)$$

なる和と積に関して可換環であり，恒等指標 1_G が乗法の単位元である．

補題 8.13 $\mathcal{I}(G,\mathcal{E}_G)$ は $\mathcal{R}(G,\mathcal{E}_G)$ のイデアルである．

証明 $\mathcal{I}(G,\mathcal{E}_G)\ni\varphi$，$\mathcal{R}(G,\mathcal{E}_G)\ni\theta$ としよう．

$$\varphi=\sum_i a_i\varphi_i{}^G\qquad(a_i\in\boldsymbol{Z},\ \ \varphi_i\in\mathrm{Irr}(E_i),\ \ E_i\in\mathcal{E}_G)$$

と書くとき，(8.44) によって

$$\theta\varphi=\sum_i a_i\theta\varphi_i{}^G=\sum_i a_i(\varphi_i\theta_{E_i})^G,\qquad\varphi_i\theta_{E_i}\in Cl_{\boldsymbol{Z}}(E_i)$$

であるから $\theta\varphi_i{}^G\in\mathcal{I}(G,\mathcal{E}_G)$．よって $\theta\varphi\in\mathcal{I}(G,\mathcal{E}_G)$ である．▌

さて，Brauer の指標定理 8.26 は，つぎの定理の系である：

定理 8.27 (Brauer) $\mathcal{I}(G,\mathcal{E}_G)\ni 1_G$．とくに $\mathcal{I}(G,\mathcal{E}_G)=Cl_{\boldsymbol{Z}}(G)=\mathcal{R}(G,\mathcal{E}_G)$．

———

補題 8.13 により，$\mathcal{I}(G,\mathcal{E}_G)\ni 1_G$ から $\mathcal{I}(G,\mathcal{E}_G)=Cl_{\boldsymbol{Z}}(G)=\mathcal{R}(G,\mathcal{E}_G)$ がでることに注意する．ここで定理 8.27 から定理 8.26 が得られることを注意しておこう．定理 8.26 の (i) は $Cl_{\boldsymbol{Z}}(G)=\mathcal{R}(G,\mathcal{E}_G)$ にほかならない．(ii) を示そう．$\mathcal{I}(G,\mathcal{E}_G)=Cl_{\boldsymbol{Z}}(G)$ より，G の任意の指標 χ は

$$\chi=\sum a_i\varphi_i{}^G\quad(a_i\in\boldsymbol{Z}),\qquad\varphi_i\in\mathrm{Irr}\,(E_i)\quad(E_i\in\mathcal{E}_G)$$

と書ける．E_i は巾零群であるから，定理 8.21 により φ_i は E_i の部分群 F_i の1次指標 λ_i の誘導指標である：$\varphi_i=\lambda_i{}^{E_i}$．よって (8.43) により

$$\chi = \sum_i a_i (\lambda_i{}^{E_i})^G = \sum_i a_i \lambda_i{}^G$$

となり，定理 8.26 の (ii) が得られる．したがって定理 8.26 は定理 8.27 を証明することに帰着された．

定理 8.27 は，最初，1947 年に Brauer により証明されたが，その証明はかなり複雑なものであった．その後

R. Brauer, J. Tate: On the characters of finite groups, Ann. of Math. **62** (1955), 1–7

において別証明が得られ，通常この証明が一般の書物では述べられている[1]．ここでは，それとは異なる証明を紹介する．それは

M. Isaacs: Character Theory of Finite Groups, Academic Press (1976)

に見られるものである．

まず基本部分群の概念を少し拡張しよう．G の部分群 F が，

$$F = PC \triangleright C, \qquad P \cap C = 1,$$
$$P = \text{或る素数 } p \text{ に対する } p \text{ 群},$$
$$C = \text{位数が } p \text{ と素な巡回群}$$

なる構造をもつとき，F を**準基本部分群**という．とくに p に言及したいときは**準 p 基本部分群**という．準 p 基本部分群の部分群は準 p 基本部分群である．$\mathcal{E}_G{}'$ によって G の準基本部分群の全体を表わそう．さて，G のいくつかの可移置換表現の指標の整係数1次結合の全体を $P(G)$ としよう：

$$P(G) = \left\{ \sum_i a_i 1_{H_i}{}^G \middle| a_i \in \boldsymbol{Z},\ H_i \text{ は } G \text{ の部分群} \right\}.$$

また，

$$P(G, \mathcal{E}_G{}') = \left\{ \sum_i a_i 1_{F_i}{}^G \middle| a_i \in \boldsymbol{Z},\ F_i \in \mathcal{E}_G{}' \right\}$$

とおく．

定理 8.28 (L. Solomon)　$P(G) = P(G, \mathcal{E}_G{}')$.

証明　段階に分けて証明する．

(α)　$P(G)$ は環，$P(G, \mathcal{E}_G{}')$ は $P(G)$ のイデアルである．

[証明]　H, K を G の部分群とするとき，$1_K{}^G = \theta$ とおくと，(8.44) により

$$1_H{}^G \cdot 1_K{}^G = \theta \cdot 1_H{}^G = \theta_H{}^G.$$

---

1) たとえば，秋月，鈴木：代数 II (岩波全書)．

ところで，Mackey 分解 (8.31) (例 8.8) により

$$\theta_H = 1_K{}^G \mid H = \sum_i 1_{\tilde{K}_i}{}^H, \qquad \tilde{K}_i = x_i K x_i{}^{-1} \cap H \subseteqq H$$

であるから，(8.43) を用いて

$$\theta_H{}^G = \sum_i (1_{\tilde{K}_i}{}^H)^G = \sum_i 1_{\tilde{K}_i}{}^G \in P(G).$$

よって $P(G)$ が環であることがわかる．とくに H として $\mathcal{E}_G'$ の元をとれば $\tilde{K}_i \in \mathcal{E}_G'$ であるから，上の推論は $P(G, \mathcal{E}_G')$ が $P(G)$ のイデアルであることを示す．▌

(β) $G \ni x$, p を素数とする．このとき $F \in \mathcal{E}_G'$ を適当にとれば，$1_F{}^G(x)$ は p で割れない．

[証明] $\langle x \rangle = P \otimes C, \quad P = p$ 群， $p \nmid |C|$

とする．$N = N_G(C)$ とおくと $x \in N$ である．N/C の Sylow p 部分群 F/C で $x \in F$ なるものをとる．F は準 p 基本部分群である．以下 $1_F{}^G(x)$ が p で割れないことを示そう．ところで $1_F{}^G(x)$ は x の G/F への作用の固定点の数である：

$$1_F{}^G(x) = (xyF = yF \text{ なる左剰余類 } yF \text{ の数}).$$

$xyF = yF$ ならば，$y^{-1}xy \in F$ より $y^{-1}Cy \subseteqq F$. このとき F が準 p 基本部分群であることに注意すれば $y^{-1}Cy = C$, すなわち $y \in N$ である．これは $1_F{}^G(x)$ が x の N/F への作用の固定点の数に等しいことを示す．ところで，$N \triangleright C$ で C は N/F の各元を固定するから，C は N の N/F への作用の核に含まれる．$\langle x \rangle / C$ は p 群だから，x の N/F への作用の軌道への分解を考えて，$[N : F] \equiv 1_F{}^G(x) \pmod{p}$ を得る．$p \nmid [N : F]$ であるから $p \nmid 1_F{}^G(x)$ である．▌

(γ) $1_G \in P(G, \mathcal{E}_G')$.

[証明] $G \ni x$ に対して，$I_x = \{f(x) \mid f \in P(G, \mathcal{E}_G')\}$ とおく．I_x は $\boldsymbol{Z}$ の部分群である．まず

(＊) $I_x = \boldsymbol{Z} \qquad (\forall x \in G)$

を示そう．実際，ある x に対して $I_x = \langle m \rangle$ $(1 \neq m \in \boldsymbol{Z})$ とすると，$p \mid m$ なる素数 p をとれば，$p \mid f(x)$ $(\forall f \in P(G, \mathcal{E}_G'))$ である．しかるに $F \in \mathcal{E}_G'$ を (β) のようにとれば，$p \nmid 1_F{}^G(x)$, $1_F{}^G \in P(G, \mathcal{E}_G')$ であるから矛盾である．(＊) により G の各元 x に対して $f_x(x) = 1$ なる $P(G, \mathcal{E}_G')$ の元 f_x が存在する．このとき

$$\prod_{x \in G} (f_x - 1_G) = 0$$

であるから，この左辺を展開して 1_G を移項すれば $1_G \in P(G, \mathcal{E}_G')$ を得る．▌

(α) と (γ) から $P(G,\mathcal{E}_G')=P(G)$ を得る. ▌

定理8.27の証明を始めよう. その要点は, L. Solomon の定理8.28を用いて, G が準基本部分群である場合に帰着させることにある.

定理8.27の証明　最初に, G 自身が基本部分群であるとき, 定理8.27は明らかに成り立つことに注意する. 以下二つの場合に分けよう.

(α)　G が準基本部分群であるとき.

$$G=PC\triangleright C,\quad P=p\text{ 群},\quad C=\text{位数が } p \text{ と素な巡回群}$$

としよう.

$$Z=C_C(P),\quad E=ZP$$

とおくと,

$$G\triangleright Z,\quad E\in\mathcal{E}_G$$

である. 最初の注意により $G\neq E$ と仮定してよい.

$1_E{}^G=1_G+\varphi$, χ を φ の既約成分とするとき $\chi\in\mathcal{I}(G,\mathcal{E}_G)$ を示せば, $1_G=1_E{}^G-\varphi\in\mathcal{I}(G,\mathcal{E}_G)$ となるから, (α) の証明は終る. 以下, $\chi\in\mathcal{I}(G,\mathcal{E}_G)$ を示そう. λ を $\varphi|C$ の既約成分としよう. まず,

$$(*)\qquad \lambda\neq 1_C,\quad Z\subseteqq \mathrm{Ker}\,\lambda$$

を示そう. $G=CE$, $C\cap E=Z$ であるから, Mackey 分解(8.31)により

$$1_C+\varphi_C=(1_E{}^G)_C=1_Z{}^C$$

である. $1_Z{}^C$ は C/Z の正則表現の指標であるから, 1_C を重複度1で含む(例8.9). よって φ_C は 1_C を含まず, とくに $\lambda\neq 1_C$ である. また $E\supseteqq Z\lhd G$ より $Z\subseteqq \mathrm{Ker}\,((1_E{}^G)_C)$, よって $Z\subseteqq\mathrm{Ker}\,\lambda$ である. つぎに

$$(**)\qquad G\neq I_G(\lambda)$$

を示そう. $T=I_G(\lambda)$, $K=\mathrm{Ker}\,\lambda$ とおく. $G=T$ と仮定して矛盾を導こう. xK $(x\in C)$ は P 不変, すなわち $y^{-1}(xK)y=xK$ $(\forall y\in P)$ である. なぜなら, λ は1次指標であるから, λ は K の異なる剰余類の上で異なる値をとるが, $G=T$ より $\lambda^y=\lambda$ $(\forall y\in P)$ であるから, xK は P 不変でなければならない. よって P の xK の上への共役による作用を考えると, P は xK の上に固定点をもつ(補題2.1). よって $Z\cap xK=C_C(P)\cap xK\neq\phi$ であるが, $Z\subseteqq K$ より $x\in K$ を得る. x は C の任意の元だから, $K=C$ となり, これは $\lambda=1_C$ を示すから, $(*)$ に反する. これで $(**)$ が示された. さて定理8.19により, $\chi=\psi^G$ なる $\psi\in\mathrm{Irr}\,(T)$ が存

在する．$(**)$により $|T|<|G|$ であるから，(α)を G の位数に関する数学的帰納法で証明することにすれば，$\psi\in\mathcal{I}(T,\mathcal{E}_T)$ と仮定してよい．このとき，(8.43)を用いて $\chi=\psi^G\in\mathcal{I}(G,\mathcal{E}_G)$ を得る．

(β) G が準基本部分群でないとき．

G の位数に関する帰納法による．H が G の真の部分群ならば，$1_H\in\mathcal{I}(H,\mathcal{E}_H)$ と仮定してよい．とくに

$$(*)\qquad 1_F\in\mathcal{I}(F,\mathcal{E}_F)\qquad (\forall F\in\mathcal{E}_G{}')$$

である．定理 8.28 により

$$1_G=\sum a_i 1_{F_i}{}^G\qquad (F_i\in\mathcal{E}_G{}',\ a_i\in\boldsymbol{Z})$$

であるが，$(*)$と(8.43)により

$$1_{F_i}{}^G\in\mathcal{I}(G,\mathcal{E}_G)$$

であるから，$1_G\in\mathcal{I}(G,\mathcal{E}_G)$ を得る．▌

Brauer の指標定理(定理 8.26)は多くの重要な応用をもつ．そのもっとも有名なものは，

(i) いわゆる Artin L 関数が複素全平面で有理型関数であること(“Artin L 関数は複素全平面で整関数であろう”というもっと強い予想がある)，

(ii) 有限群 G の複素数体上の任意の表現は，その行列表示を適当にとれば，行列の成分が有理数体に 1 の原始 n 乗根 $(n=|G|)$ を添加した体に含まれるようにできること

などである．これらは，いずれも定理 8.26 の(ii)の応用であるが，本書では省く．(i)については，岩波講座基礎数学“数論”を，(ii)については，秋月，鈴木：代数 II (岩波全書)を参照されたい．本書では，以下定理 8.26 の(i)の二つの応用を述べる．

b) Brauer による一定理

ここでは，Brauer の指標定理(定理 8.26 の(i))の応用として，つぎの定理を証明する．この定理は本来モジュラー表現論で証明されたものであり，理論的にもその方面から理解するのが自然である．

定理 8.29 (Brauer) p を素数，χ を G の既約指標で $|G|/\chi(1)$ が p で割れないものとする．このとき，位数が p で割れる G の任意の元 x に対して $\chi(x)=0$ である．

証明　$G\ni x$ に対して

$$\theta(x)=\begin{cases}\chi(x) & (x \text{ の位数が } p \text{ と素のとき}),\\ 0 & (x \text{ の位数が } p \text{ で割れるとき})\end{cases}$$

とおく．明らかに θ は G の類関数である．θ が一般指標であることを示そう．それには定理8.26の(i)により

$$(*)\qquad E\in\mathcal{E}_G\Longrightarrow \theta\,|\,E\in Cl_{\boldsymbol{Z}}(E)$$

を示せばよい．$p\nmid|E|$ ならば，θ の定義により $\theta\,|\,E=\chi\,|\,E$ であるから，これは明らかである．よって $p\,|\,|E|$ としよう．このとき，E は巾零群だから

$$E=P\otimes Q,\qquad P=p\text{ 群}\neq 1,\qquad p\nmid|Q|$$

と書ける．また，θ は類関数であるから，

$$\theta\,|\,E=\sum_{\zeta\in\mathrm{Irr}(E)}(\theta\,|\,E,\zeta)_E\,\zeta$$

と書けるから，$(*)$を示すには，

$$(**)\qquad (\theta\,|\,E,\zeta)_E\in\boldsymbol{Z}$$

を示せばよい．θ の定義と E の構造に注意して

$$\begin{aligned}(\theta\,|\,E,\zeta)_E&=\frac{1}{|E|}\sum_{y\in E}\theta(y)\overline{\zeta(y)}=\frac{1}{|E|}\sum_{y\in Q}\chi(y)\overline{\zeta(y)}\\&=\frac{|Q|}{|E|}\frac{1}{|Q|}\sum_{y\in Q}\chi(y)\overline{\zeta(y)}=\frac{1}{|P|}(\chi\,|\,Q,\zeta\,|\,Q)_Q\end{aligned}$$

であるから，

$$(***)\qquad |P|(\theta\,|\,E,\zeta)_E\in\boldsymbol{Z}$$

を得る．さて，$G\ni x$ に対して

$$\omega(x)=\frac{|K_x|\chi(x)}{\chi(1)}\qquad (K_x \text{ は } x \text{ を含む共役類})$$

とおくと，定理8.12により $\omega(x)$ は代数的整数である．

$$\begin{aligned}|E|(\theta\,|\,E,\zeta)_E&=\sum_{y\in Q}\chi(y)\overline{\zeta(y)}\\&=\frac{\chi(1)}{|G|}\sum_{y\in Q}\omega(y)\overline{\zeta(y)}|C_G(y)|\qquad\left(|K_y|=\frac{|G|}{|C_G(y)|}\text{ に注意}\right)\\&=\frac{|P|\chi(1)}{|G|}\sum_{y\in Q}\omega(y)\overline{\zeta(y)}[C_G(y):P]\\&\qquad\qquad (C_G(y)\supseteqq P\ (\forall y\in Q)\text{ に注意})\end{aligned}$$

であるから

$$\frac{|G||Q|}{\chi(1)}(\theta\,|\,E,\zeta)_E=\sum_{y\in Q}\omega(y)\overline{\zeta(y)}[C_G(y):P],\qquad |E|=|P||Q|$$

を得る．この式の右辺は代数的整数であるから，左辺の有理数は整数でなければならない：

$$(****)\qquad \frac{|G||Q|}{\chi(1)}(\theta\,|\,E,\zeta)_E\in \boldsymbol{Z}$$

となる．ところで，$|G||Q|/\chi(1)$ は p と素であるから，$(***)$ と $(****)$ から $(\theta\,|\,E,\zeta)_E\in\boldsymbol{Z}$ すなわち $(**)$ が得られ，θ は G の一般指標となる．とくに $(\theta,\theta)_G\in\boldsymbol{Z}$ である．一方，θ の定義により

$$0\leqq(\theta,\theta)_G\leqq(\chi,\chi)_G\leqq 1,\qquad \theta(1)=\chi(1)>0$$

であるから $(\theta,\theta)_G=1$ でなければならない．このとき補題 8.12 により，θ は G の既約指標であるが，直交関係により $\theta=\chi$ でなければならない．▌

例 8.18 $PGL(2,q)$ は q 個の元をもつ有限体 F_q の上の射影直線 $\boldsymbol{P}$ の上に 2 重可移に作用する (例 2.5)．$|\boldsymbol{P}|=q+1$ であるから，§8.4, b)，例題 8.2 により，$PGL(2,q)$ は q 次の既約指標 χ をもつ．$|PGL(2,q)|=q(q^2-1)$ であるから，$q=p^a$ とするとき，χ は定理 8.29 の仮定を満たす．よって $PGL(2,q)$ の位数が p で割れる元 x に対して $\chi(x)=0$．たとえば $x=\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}$ $(\beta\neq 0)$ とすると，$\chi\left(\begin{bmatrix}\alpha & \beta\\ 0 & \alpha\end{bmatrix}\right)=0$ である．

問 8.23 P を G の Sylow p 部分群，χ は G の既約指標で $\chi(x)=0$ $(1\neq\forall x\in P)$ とする．このとき，$|G|/\chi(1)$ は p で割れないことを示せ．

c) $GL(2,q)$, $SL(2,q)$ の既約指標

この項では，Brauer の指標定理 (定理 8.26) の応用として，つぎの補題 8.14 を証明し，これを用いて $GL(2,q)$ の既約指標を決定する．さらに，$GL(2,q)$ の既約指標から，Clifford の定理 8.18 を用いて $SL(2,q)$ の既約指標を決定する．

補題 8.14 (J. A. Green) q^2 個の元からなる有限体の乗法群の生成元を ρ とする．また θ を巡回群 $\langle\rho\rangle$ から複素数体の乗法群への任意の準同型とするとき，つぎのように定義される $GL(2,q)$ の類関数 φ は，$GL(2,q)$ の一般指標である：

$$GL(2,q)\ni A \text{ の固有値が } \rho^i,\rho^j \text{ のとき } \varphi(A)=\theta(\rho^i)+\theta(\rho^j).$$

注意 実は，この補題は任意の有限群とその有限体上の任意の表現に対して一般化される．この一般的定理の証明も，もちろん Brauer の指標定理に基づくもので，それほど難

しいものではない．実際，その一般的証明の方が，後に与える補題 8.14 の証明よりすっきりしていることも事実であるが，本書では少し準備不足のため割愛することにする．興味のある読者は，

J. A. Green: The characters of the finite general linear groups, Trans. Amer. Math. Soc. **80** (1955), 402–447

の中の定理1を参照されたい．なお，この論文において，J. A. Green は $GL(n, q)$ のすべての既約指標を決定しており，そこでは上の補題 8.14（の一般化）が重要な役割を演じている．

さて，補題 8.14 を証明する前に，$GL(2, q)$ の共役類を決定しよう．

補題 8.15　$G=GL(2, q)$ はつぎの性質をもつ位数 q^2-1 の元 B をもつ：

(i)　$\langle B\rangle \supseteqq Z$．ここで Z は $GL(2, q)$ のスカラー行列の全体で，$GL(2, q)$ の中心である，

(ii)　$\langle B\rangle - Z \ni X$, $YXY^{-1}=X^r$ $(Y \in G)$ ならば，$X^r=X$ または X^q,

(iii)　$\langle B\rangle - Z \ni X$ ならば，$C_G(X)=\langle B\rangle$,

(iv)　$|N_G(\langle B\rangle)| = 2(q^2-1)$.

証明　F を q 個の元をもつ有限体，K を F の2次拡大とする．K は F 上2次元線型空間である．したがって $G=GL(2, q)$ を $GL(K)$ と同一視する．K の乗法群 K^* は位数 q^2-1 の巡回群だから，その生成元を ρ とすると，$\delta=\rho^q$ は F の乗法群 F^* の生成元である：$K^*=\langle\rho\rangle$, $F^*=\langle\delta\rangle$．さて K から K への写像 B を

$$B(\gamma) = \rho\gamma \qquad (\gamma \in K)$$

によって定義すると，明らかに $B \in GL(K)$，B の位数は q^2-1 である．また $\langle B^{q+1}\rangle$ は $GL(K)$ のスカラー変換からなる位数 $q-1$ の部分群であるから $\langle B\rangle \supseteqq Z=\langle B^{q+1}\rangle$．すなわち (i) が成り立つ．$A \in GL(K)$ を

$$A(\gamma) = \gamma^q \qquad (\gamma \in K)$$

によって定義すると，

$$A^2 = 1, \qquad A^{-1}BA = B^q$$

であることが容易にわかる．したがって

$$\langle A, B\rangle \subseteqq N_G(\langle B\rangle)$$

である．

$$\langle B\rangle - Z \ni X, \qquad YXY^{-1} = X^r \quad (Y \in G)$$

としよう．$X=B^i$，$\tau=\rho^i$ とおくと

$$X(\gamma)=\tau\gamma \qquad (\gamma\in K)$$

で，$\langle B\rangle-Z\ni X$ より $\tau\notin F$ である．したがって，$1,\tau$ は K の F 上の基底となり，K の元は

$$a+b\tau \qquad (a,b\in F)$$

の形に書ける．さて $Y(\gamma\mu)$ $(\gamma,\mu\in K)$ を計算しよう．$\gamma=a+b\tau$ とすると

$$\begin{aligned}Y(\gamma\mu) &= Y(a\mu+b\tau\mu)=aY(\mu)+bYX(\mu)\\ &= aY(\mu)+bX^rY(\mu)=(a+b\tau^r)Y(\mu)\end{aligned}$$

である．ここで，K から K への写像 φ を

$$\varphi(a+b\tau)=a+b\tau^r$$

によって定義すると，$\varphi\in GL(K)$ で，上の計算から

$$Y(\gamma\mu)=\varphi(\gamma)Y(\mu)$$

である．とくに

$$\begin{aligned}Y(\gamma\mu) &= Y(\gamma\mu\cdot 1)=\varphi(\gamma\mu)Y(1),\\ \varphi(\gamma)Y(\mu) &= \varphi(\gamma)Y(\mu\cdot 1)=\varphi(\gamma)\varphi(\mu)Y(1)\end{aligned}$$

から $\varphi(\gamma\mu)=\varphi(\gamma)\varphi(\mu)$ を得る．よって φ は体 K の F 上の自己同型となり，$\varphi(\gamma)=\gamma$ または γ^q である．よって $Y(\gamma)=\gamma Y(1)$ または $\gamma^qY(1)$ となり，これは $Y\in\langle A,B\rangle$ を示し，(ii)，(iv) がわかる．$YXY^{-1}=X$ とすると，$\varphi(\gamma)=\gamma$，$Y(\gamma)=\gamma Y(1)$ であるから $Y\in\langle B\rangle$ となり (iii) が成り立つ．▌

問 8.24　$GL(2,q)$ の任意の位数 q^2-1 の部分群は，補題 8.15 における $\langle B\rangle$ と共役であることを示せ．

問 8.25　つぎのことを示せ：

(i)　$GL(n,q)$ は位数 q^n-1 の元 B を含む．

(ii)　$m|n$，$m\neq n$ なる m に対して $\langle B\rangle$ の位数 q^m-1 の部分群をとり，それらの全体を S とするとき

$$\langle B\rangle-\bigcup_{S\ni H}H\ni X,\quad YXY^{-1}=X^r\ (Y\in GL(n,q))\Longrightarrow X^r=X^{q^i}\quad (i\in \boldsymbol{Z}).$$

(iii)　$\langle B\rangle-\bigcup_{S\ni H}H\ni X\Longrightarrow C_G(X)=\langle B\rangle.$

［ヒント］　補題 8.15 の証明の真似をせよ．

定理 8.30　δ を q 個の元からなる有限体の乗法群の生成元，B を補題 8.15 に

おける $GL(2,q)$ の元,

$$Z=\begin{bmatrix}\delta & 0\\ 0 & \delta\end{bmatrix},\qquad P=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},\qquad D_{ij}=\begin{bmatrix}\delta^i & 0\\ 0 & \delta^j\end{bmatrix}\quad (i,j\in \boldsymbol{Z})$$

とおく．このとき，つぎのことが成り立つ:

(i) $GL(2,q)$ の共役類は四つの族 I, II, III, IV から成り，各族に属する共役類の代表元は,

I　Z^i　$(0\leqq i<q-1)$,

II　PZ^i　$(0\leqq i<q-1)$,

III　D_{ij}　$(0\leqq i<j<q-1)$,

IV　B^i　$(0\leqq i<q^2-1,\ q+1\nmid i.$ さらに i は $iq\equiv i'\ (\mathrm{mod}\ q^2-1)$ なる i,i' の一方のみをとる$)$.

(ii) 各族に含まれる共役類の数は，それぞれ

$$q-1,\quad q-1,\quad \frac{(q-1)(q-2)}{2},\quad \frac{q^2-q}{2}.$$

(iii) 各族に含まれる共役類の元の数は，それぞれ

$$1,\quad q^2-1,\quad q(q+1),\quad q(q-1).$$

証明　位数および固有値を比べて，(i) にあげた

$$Z^i,\quad PZ^i,\quad D_{ij},\quad B^i\qquad (i,j\ \text{は (i) のように動く})$$

が，互いに共役でないことは明らかであろう．また，これらの元の中心化群を，最初の3種類に対しては行列の計算，B^i については補題8.15から計算すると，その位数は，それぞれ

$$q(q^2-1)(q-1)=|GL(2,q)|,\quad q(q-1),\quad (q-1)^2,\quad q^2-1$$

であるから，これらの元を代表元とする共役類の元の数は

$$1,\quad q^2-1,\quad q(q+1),\quad q(q-1)$$

となる．よってこれらの共役類のどれかに含まれる $GL(2,q)$ の元の総数は，i,j の動く範囲に注意して

$$1\times(q-1)+(q^2-1)\times(q-1)+q(q+1)\times\frac{(q-1)(q-2)}{2}+q(q-1)\times\frac{q^2-q}{2}$$

となり，これは $GL(2,q)$ の位数 $q(q^2-1)(q-1)$ に等しい．よって，(i), (ii), (iii) が同時に証明されたことになる．∎

一般に有限群 G のすべての基本部分群をみつけるには，つぎのようにすればよい：G の共役類の代表元 $x_1, x_2, \cdots, x_h$ を定め，各 i に対して x_i の位数を割らない素数 $p_{ij}\,(j=1,2,\cdots,n_i)$ と，$C_G(x_i)$ の Sylow p_{ij} 部分群 P_{ij} を一つとる．このとき，G の任意の基本部分群は

$$\langle x_i\rangle\otimes P_{ij} \qquad (1\leqq i\leqq h,\ 1\leqq j\leqq n_i)$$

の部分群と共役である．したがって，Brauer の指標定理 (定理 8.26) を用いて G の類関数 φ が一般指標であることをみるには，φ の $\langle x_i\rangle\otimes P_{ij}$ への制限が $\langle x_i\rangle\otimes P_{ij}$ の一般指標であることをみれば十分である．

さて $GL(2,q)$ の基本部分群を調べよう．定理 8.30 で用いた記号のほかに，

$$U=\left\{\begin{bmatrix}1 & \alpha\\ 0 & 1\end{bmatrix}\middle|\,\alpha\in F_q\right\}, \qquad D=\{D_{ij}\,|\,i,j\in \boldsymbol{Z}\}$$

とおく．このとき，$GL(2,q)$ の任意の基本部分群は，つぎにあげる部分群の部分群に共役であることがわかる：

(α) $q=2^n$ のとき．

$$\langle Z\rangle\otimes U, \quad D, \quad \langle B\rangle.$$

(β) $q\equiv 1 \pmod 4$ のとき．

$$\langle Z\rangle\otimes U, \quad \left\langle\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, D\right\rangle, \quad \langle B\rangle.$$

(γ) $q\equiv -1 \pmod 4$ のとき．

$$\langle Z\rangle\otimes U, \quad D, \quad N_G(\langle B\rangle)=\langle A, B\,|\,A^2=B^{q^2-1}=1,\ A^{-1}BA=B^q\rangle.$$

実際，定理 8.30 であげた PZ^i, D_{ij}, B^i の中心化群は，それぞれ $\langle Z\rangle\otimes U, D, \langle B\rangle$ に含まれる．また $Z^i\in Z(GL(2,q))$ については，上にあげた部分群がすべて $\langle Z\rangle$ を含むから，$|GL(2,q)|$ を割る各素数について，$GL(2,q)$ の Sylow 部分群が上にあげた部分群のどれかに含まれればよい．これは $|GL(2,q)|=q(q^2-1)(q-1)$ と (α), (β), (γ) にあげた部分群の位数を比べれば容易に確かめることができる ((α), (β), (γ) の区別は，Sylow 2 部分群を調べるときに起ることに注意)．

補題 8.14 の証明 最初に，$GL(2,q)\ni A$ の固有値 ρ^i, ρ^j に対して $\psi(A)=\theta(\rho^i)\theta(\rho^j)$ によって定義される類関数は $\psi(A)=\theta(\det A)$ であるから，$GL(2,q)$ の 1 次指標であることに注意する．また，θ は $\langle\rho\rangle$ から $\boldsymbol{C}^*$ への同型であると仮定してよい．なぜなら，θ が $\langle\rho\rangle$ から $\boldsymbol{C}^*$ への同型であるとき，$\langle\rho\rangle$ から $\boldsymbol{C}^*$ へ

の任意の準同型は θ^k $(0\leqq k\in \boldsymbol{Z})$ と書け，さらによく知られた対称式の性質により $\theta^k(\rho^i)+\theta^k(\rho^j)$ は，$\theta(\rho^i)\theta(\rho^j)$ と $\theta(\rho^i)+\theta(\rho^j)$ の整係数多項式となるからである．したがって以下 θ は $\langle\rho\rangle$ から $\boldsymbol{C}^*$ への同型であると仮定する．よって $\theta(\rho)=\eta$ とおくと，η は1の原始 q^2-1 乗根である．さて，$\varphi(A)=\theta(\rho^i)+\theta(\rho^j)$ が $GL(2,q)$ の一般指標であることをみるには，上の (α), (β), (γ) であげた部分群への φ の制限が，その部分群の一般指標であることを確かめればよい．

(α) $q=2^n$ のとき．

$\langle Z\rangle\otimes U, D, \langle B\rangle$ への φ の制限が，いずれもこれら Abel 群の二つの1次指標の和であることは明らかである．

(β) $q\equiv 1 \pmod 4$ のとき．

$\langle Z\rangle\otimes U$, $\langle B\rangle$ への φ の制限については，(α) と同様である．D の1次指標 φ_0 をつぎのように定義する：

$$\varphi_0\left(\begin{bmatrix}\delta^i & 0\\ 0 & \delta^j\end{bmatrix}\right)=\eta^{(q+1)(i+j)}.$$

このとき，φ_0 の $\left\langle\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, D\right\rangle$ への誘導指標が φ のこの部分群への制限と一致することは容易にわかる．

(γ) $q\equiv -1 \pmod 4$ のとき．

$\langle Z\rangle\otimes U, D$ への φ の制限については，(α) のときと同様である．φ の $N_G(\langle B\rangle)=\langle A, B\mid A^2=B^{q^2-1}=1,\ A^{-1}BA=B^q\rangle$ への制限を考えよう．φ_1 を $\langle B\rangle$ の $\varphi_1(B)=\eta$ によって定義される1次指標とする．このとき，φ_1 の $N_G(\langle B\rangle)$ への誘導指標 $\varphi_1{}^*$ を計算すると，

$$\varphi_1{}^*(B^j)=\eta^j+\eta^{jq},\qquad \varphi_1{}^*(AB^j)=0$$

である．$\varphi_1{}^*=\varphi\mid N_G(\langle B\rangle)$ であることを示そう．B の固有値は ρ, ρ^q と仮定してよいから，$\varphi_1{}^*(B^j)=\varphi(B^j)$ は明らかである．したがって $\varphi_1{}^*=\varphi\mid N_G(\langle B\rangle)$ をみるには，θ が同型であることに注意して，AB^j の固有値が $\pm\rho^i$ $(\exists i\in \boldsymbol{Z})$ であることをみれば十分である．F_q の適当な拡大体 L をとれば，B は $\begin{bmatrix}\rho & 0\\ 0 & \rho^q\end{bmatrix}$ に変換される．このとき

$$A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}\qquad (a,b,c,d\in L)$$

とすると，$BA=AB^q$ より $a=d=0$，すなわち A の固有値は $\pm\rho^i$ $(i\in \boldsymbol{Z})$ であ

る. ▌

定理 8.31 (i) $GL(2,q)$ の既約指標は, 四つの族 I, II, III, IV から成り, 各族に属する既約指標の次数および個数はつぎの通りである:

I $q-1$ 個の 1 次指標 $L_n(1)$ $(0\leqq n<q-1)$,

II $q-1$ 個の q 次指標 $R_n(q)$ $(0\leqq n<q-1)$,

III $(q-1)(q-2)/2$ 個の $q+1$ 次指標 $X_{m,n}(q+1)$ $(0\leqq m<n<q-1)$,

IV $q(q-1)/2$ 個の $q-1$ 次指標 $Y_n(q-1)$ $(0\leqq n<q^2-1,\ q+1\nmid n$, さらに $n\equiv n'q\ (\mathrm{mod}\ q^2-1)$ なる n, n' の一方のみをとる).

(ii) $GL(2,q)$ の共役類の代表元は定理 8.30 の通りとする. η を 1 の原始 q^2-1 乗根, $\eta^{q+1}=\varepsilon$ とおくと, 既約指標の値はつぎのようになる:

	Z^i	PZ^i	D_{ij}	B^i
$L_n(1)$	ε^{2ni}	ε^{2ni}	$\varepsilon^{n(i+j)}$	ε^{ni}
$R_n(q)$	$q\varepsilon^{2ni}$	0	$\varepsilon^{n(i+j)}$	$-\varepsilon^{ni}$
$X_{m,n}(q+1)$	$(q+1)\varepsilon^{(m+n)i}$	$\varepsilon^{(m+n)i}$	$\varepsilon^{mi+nj}+\varepsilon^{ni+mj}$	0
$Y_n(q-1)$	$(q-1)\varepsilon^{ni}$	$-\varepsilon^{ni}$	0	$-(\eta^{ni}+\eta^{nqi})$

証明 ρ を $F_{q^2}{}^*$ ($=q^2$ 個の元からなる有限体の乗法群) の生成元, $\rho^{q+1}=\delta$ とおくと δ は $F_q{}^*$ の生成元である. θ_n を $\langle\rho\rangle$ から $\boldsymbol{C}^*$ への $\theta_n(\rho)=\eta^n$ なる準同型とすると, $X_n(1)$ は $X_n(1)(A)=\theta_n(\det A)$ $(A\in GL(2,q))$ によって定義される $GL(2,q)$ の 1 次指標 $L_n(1)$ である.

$$T=\left\{\begin{bmatrix}\delta^i & \beta\\ 0 & \delta^j\end{bmatrix}\middle|\, 0\leqq i,j<q-1,\ \beta\in F_q\right\}$$

なる $GL(2,q)$ の部分群を考える. T の位数は $q(q-1)^2$ である. 任意の整数 m, n に対して

$$\varphi_{m,n}\left(\begin{bmatrix}\delta^i & \beta\\ 0 & \delta^j\end{bmatrix}\right)=\varepsilon^{mi+nj}$$

なる T の 1 次指標 $\varphi_{m,n}$ を定義する. $\varphi_{m,n}$ の G への誘導指標 $\varphi_{m,n}{}^*$ を計算しよう. まず $Z^i\in Z(G)$ であるから,

$$\varphi_{m,n}{}^*(Z^i)=(q+1)\varepsilon^{(m+n)i}$$

である. $\varphi_{m,n}{}^*(PZ^i), \varphi_{m,n}{}^*(D_{ij}), \varphi_{m,n}{}^*(B^i)$ を計算するために G の F_q 上の 1 次元射影空間 $\boldsymbol{P}$ (F_q 上の 2 項列ベクトルからなる F_q 上の 2 次元線型空間の 1 次元

部分空間全体)への自然な作用(例2.3)を考える．このとき，T はこの作用の1点 $\left(\begin{bmatrix}\alpha\\0\end{bmatrix}(\alpha\in F_q)\text{ なる1次元部分空間}\right)$ の固定部分群である．$D_{ij}\,(i<j)$ は $\boldsymbol{P}$ のちょうど2点(D_{ij} の固有値 δ^i,δ^j に属する固有空間)を固定するから，G/T のちょうど二つの左剰余類を固定する．その一つは明らかに T であり，他の一つは $\begin{bmatrix}0&1\\1&0\end{bmatrix}^{-1}D_{ij}\begin{bmatrix}0&1\\1&0\end{bmatrix}=D_{ji}\in T$ より，$\begin{bmatrix}0&1\\1&0\end{bmatrix}T$ である．よって

$$\begin{aligned}\varphi_{m,n}{}^*(D_{ij}) &= \varphi_{m,n}(D_{ij})+\varphi_{m,n}(D_{ji})\\ &= \varepsilon^{mi+nj}+\varepsilon^{ni+mj}\end{aligned}$$

である．同様に PZ^i は $\boldsymbol{P}$ のちょうど1点(固有値 δ^i に属する固有空間)を固定するから，PZ^i は G/T のちょうど一つの左剰余類を固定する．それは明らかに T であるから，

$$\varphi_{m,n}{}^*(PZ^i) = \varepsilon^{(m+n)i}$$

である．$B^i\,(q+1\nmid i)$ の $\boldsymbol{P}$ への作用は固定点をもたないから(B^i は $q+1\nmid i$ のとき，固有値が F_q に含まれないことに注意)，B^i は G/T のどの左剰余類も固定しない．よって

$$\varphi_{m,n}{}^*(B^i) = 0 \qquad (q+1\nmid i)$$

である．さて内積 $(\varphi_{m,n}{}^*, \varphi_{m,n}{}^*)$ を計算すると[1]，

$$(\varphi_{m,n}{}^*, \varphi_{m,n}{}^*) = \begin{cases}1 & (m\neq n),\\ 2 & (m=n)\end{cases}$$

がわかる．よって $m\neq n$ のとき，$\varphi_{m,n}{}^*$ は G の既約指標である．これから $(q-1)(q-2)/2$ 個の $q+1$ 次既約指標 $X_{m,n}(q+1)$ が得られる．また $m=n$ のとき，$(\varphi_{m,m}{}^*, L_m(1))=1$ となるから，$\varphi_{m,m}{}^*=L_m(1)+R_m(q)$ とおくと，$R_m(q)$ は既約指標である．よって $q-1$ 個の q 次既約指標 $R_m(q)$ が得られた．さて，補題8.14を用いて $q-1$ 次の既約指標を構成しよう．補題8.14により任意の整数 n に対して

$$\begin{aligned}\Phi_n(Z^i) &= \eta^{ni(q+1)}+\eta^{ni(q+1)}, &\quad \Phi_n(PZ^i) &= \eta^{ni(q+1)}+\eta^{ni(q+1)},\\ \Phi_n(D_{ij}) &= \eta^{ni(q+1)}+\eta^{nj(q+1)}, &\quad \Phi_n(B^i) &= \eta^{ni}+\eta^{niq}\end{aligned}$$

なる Φ_n は G の一般指標である．このとき，

$$X_{0,n}(q+1)-\Phi_n = Y_n(q-1)$$

1) 内積の計算は読者自ら試みられたい．定理8.30を用いて直接計算すればよい．

とおくと，$q+1 \nmid n$ のとき $(Y_n(q-1), Y_n(q-1))=1$ である．$Y_n(q-1)(1)>0$ であるから，補題 8.12 により $Y_n(q-1)$ は $q+1 \nmid n$ のとき $GL(2,q)$ の $q-1$ 次既約指標である．$n \equiv n'$ または $n'q \pmod{q^2-1}$ のとき，$Y_n(q-1)=Y_{n'}(q-1)$ に注意すれば，このようにして $(q^2-q)/2$ 個の $q-1$ 次既約指標が得られる．いままでに得られた既約指標の数は，$GL(2,q)$ の共役類の数に等しいから，$GL(2,q)$ の既約指標は既に得られたものに限ることがわかる．∎

注意 上の証明で述べた $q-1$ 次の既約指標の構成は，少し天下り的な感じを与えるが，J. A. Green によるこの方法は $GL(n,q)$ $(n>2)$ の既約指標の構成にも通用する一般的なものである．この方法にはよらずに $GL(2,q)$ の $q-1$ 次の既約指標を構成するには，巡回部分群 $\langle B\rangle$ の 1 次指標の誘導指標を作り，それを既約指標に分解するのであるが，それはあまり見通しのよいものではない．

最後に，$SL(2,q)$ の共役類と既約指標を決定しよう．$q=2^n$ のときは，

$$GL(2,2^n)=\langle Z\rangle \otimes SL(2,2^n)$$

であるから話は簡単である．$SL(2,2^n)$ の共役類の代表元は，

$$\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad P=\begin{bmatrix}1&1\\0&1\end{bmatrix},\quad D_i=\begin{bmatrix}\delta^i&0\\0&\delta^{-i}\end{bmatrix}\ \left(1\leqq i\leqq\frac{q-2}{2}\right),\quad C^i\ \left(1\leqq i\leqq\frac{q}{2}\right)$$

である．ただし，C は B を定理 8.30 における位数 q^2-1 の元とするとき，$C=B^{q-1}$ である．また既約指標は $GL(2,2^n)$ の各既約指標を $SL(2,2^n)$ に制限して得られる．詳しくは読者にまかせることにして，指標表を書いておこう．

$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$	$\begin{bmatrix}\delta^i&0\\0&\delta^{-i}\end{bmatrix}$	C^i	
1	1	1	1	
q	0	1	-1	
$q+1$	1	$\varepsilon^{ni}+\varepsilon^{-ni}$	0	$\left(1\leqq n\leqq\frac{q-2}{2}\right)$
$q-1$	-1	0	$-(\sigma^{mi}+\sigma^{-mi})$	$\left(1\leqq m\leqq\frac{q}{2}\right)$

ただし，$\sigma=\eta^{q-1}$ である．なお，後の §8.7 においてまったく別の方法で $SL(2,2^n)$ の既約指標を求めるであろう（§8.7，例 8.20 参照）．

以下，q は奇数と仮定する．定理 8.30-8.31 の記号はそのまま用いることにして，そのほかに ν を $F_q{}^*$ の非平方数の一つとして固定する．また，

$$Z_0=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\qquad P'=\begin{bmatrix}1 & \nu\\ 0 & 1\end{bmatrix},\qquad C=B^{q-1},\qquad D=\begin{bmatrix}\delta & 0\\ 0 & \delta^{-1}\end{bmatrix}$$

とおく.

定理 8.32　(i)　$SL(2,q)$ ($q=$奇数) の各共役類の代表元とその元の数はつぎの通りである:

$$\begin{array}{cccccccc} E, & Z_0, & P, & PZ_0, & P', & P'Z_0, & D^i\left(1\leqq i\leqq\dfrac{q-3}{2}\right), & C^i\left(1\leqq i\leqq\dfrac{q-1}{2}\right) \\ 1 & 1 & \dfrac{q^2-1}{2} & \dfrac{q^2-1}{2} & \dfrac{q^2-1}{2} & \dfrac{q^2-1}{2} & q(q+1) & q(q-1). \end{array}$$

(ii)　$q\equiv 1\ (\mathrm{mod}\ 4)$ ならば, P と P^{-1} は $SL(2,q)$ の同じ共役類に属する. $q\equiv -1\ (\mathrm{mod}\ 4)$ ならば, P^{-1} は $SL(2,q)$ で P' と共役である.

証明　$G=GL(n,q)$, $G_1=\langle Z\rangle SL(2,q)\left(Z=\begin{bmatrix}\delta & 0\\ 0 & \delta\end{bmatrix}\right)$ とおく. $[G:G_1]=2$, G_1 は行列式が $F_q{}^*$ の元の平方である G の元の全体である. $SL(2,q)\ni X$ とするとき, つぎの (＊), (＊＊) は容易に確かめられる:

(＊)　$C_G(X)\subsetneqq G_1$ ならば, X を含む G の共役類は $SL(2,q)$ の共役類でもある.

(＊＊)　$C_G(X)\subseteqq G_1$ ならば, X を含む G の共役類は, $SL(2,q)$ で同じ個数の元からなる二つの共役類に分れる. $G-G_1\ni Y$ とすると, X, YXY^{-1} がその代表元である.

さて, 定理 8.30 であげた $GL(2,q)$ の共役類の代表元で $SL(2,q)$ に含まれるものは

$$E=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad Z_0=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\quad P=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix},\quad PZ_0=\begin{bmatrix}-1 & -1\\ 0 & -1\end{bmatrix},$$

$$D^i=\begin{bmatrix}\delta^i & 0\\ 0 & \delta^{-i}\end{bmatrix},\quad C^i$$

である. $G_1\supseteqq C_G(P)=C_G(PZ_0)=\left\{\begin{bmatrix}\alpha & *\\ 0 & \alpha\end{bmatrix}\middle|\,\alpha\in F_q{}^*\right\}$ であるから, (＊＊) により, P, PZ_0 を代表元とする G の共役類は $SL(2,q)$ で二つの共役類に分れる. $\begin{bmatrix}\nu & 0\\ 0 & 1\end{bmatrix}\in G-G_1$ であるから, P と $P'=\begin{bmatrix}\nu & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}\nu & 0\\ 0 & 1\end{bmatrix}^{-1}$ および PZ_0 と $P'Z_0$ がそれらの共役類の代表元である. つぎに

$$C_G(D^i), C_G(C^i)\subsetneqq G_1$$

より，(*)を用いて D^i, C^i を代表元とする G の共役類は $SL(2,q)$ の共役類でもある．以上により定理 8.32 の (i) が示された．$q\equiv 1\ (\mathrm{mod}\ 4)$ ならば，$\alpha^2=-1$ なる $\alpha\in F_q$ が存在する．このとき，

$$\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix}P\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix}^{-1}=\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}=P^{-1}$$

である．$q\equiv -1\ (\mathrm{mod}\ 4)$ ならば，-1 は F_q で非平方数であるから $\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\notin G_1$．よって(**)により P と $\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}P\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}^{-1}=P^{-1}$ は，$SL(2,q)$ で共役ではない．▮

定理 8.33 $SL(2,q)$ (q＝奇数) の既約指標はつぎの通りである．ただし $e=(-1)^{(q-1)/2}$ とおく．また，$PZ_0, P'Z_0$ における既約指標 χ の値（つぎの表にはでていない）は，

$$\chi(PZ_0)=\frac{\chi(Z_0)}{\chi(1)}\chi(P),\qquad \chi(P'Z_0)=\frac{\chi(Z_0)}{\chi(1)}\chi(P')$$

から得られる．

	E	Z_0	P	P'	D^i	C^i	
1_G	1	1	1	1	1	1	
R	q	q	0	0	1	-1	
X_m	$q+1$	$(-1)^m(q+1)$	1	1	$\varepsilon^{mi}+\varepsilon^{-mi}$	0	$\left(1\leqq m\leqq\frac{q-3}{2}\right)$
Y_n	$q-1$	$(-1)^n(q-1)$	-1	-1	0	$-(\sigma^{ni}+\sigma^{-ni})$	$\left(1\leqq n\leqq\frac{q-1}{2}\right)$
ξ_1	$\frac{q+1}{2}$	$\frac{e(q+1)}{2}$	$\frac{1+\sqrt{eq}}{2}$	$\frac{1-\sqrt{eq}}{2}$	$(-1)^i$	0	
ξ_2	$\frac{q+1}{2}$	$\frac{e(q+1)}{2}$	$\frac{1-\sqrt{eq}}{2}$	$\frac{1+\sqrt{eq}}{2}$	$(-1)^i$	0	
η_1	$\frac{q-1}{2}$	$-\frac{e(q-1)}{2}$	$\frac{-1+\sqrt{eq}}{2}$	$\frac{-1-\sqrt{eq}}{2}$	0	$(-1)^{i+1}$	
η_2	$\frac{q-1}{2}$	$-\frac{e(q-1)}{2}$	$\frac{-1-\sqrt{eq}}{2}$	$\frac{-1+\sqrt{eq}}{2}$	0	$(-1)^{i+1}$	

証明 定理 8.31 で得られた，$GL(2,q)$ の既約指標 $L_n(1), R_n(q), X_{m,n}(q+1), Y_n(q-1)$ の $SL(2,q)$ への制限は，

	E	Z_0	P	D^i	C^i	
L	1	1	1	1	1	
R	q	q	0	1	-1	
X_m	$q+1$	$(-1)^m(q+1)$	1	$\varepsilon^{mi}+\varepsilon^{-mi}$	0	$\left(1\leqq m\leqq\dfrac{q-1}{2}\right)$
Y_n	$q-1$	$(-1)^n(q-1)$	-1	0	$-(\sigma^{ni}+\sigma^{-ni})$	$\left(1\leqq n\leqq\dfrac{q+1}{2}\right)$

となる．ただし，$X_{m,n}(q+1)$ の $SL(2,q)$ への制限では，$n-m$ をあらためて m とおく．さて，これらの指標の内積を計算すると，

$$(X_{(q-1)/2}, X_{(q-1)/2})=2, \qquad (Y_{(q+1)/2}, Y_{(q+1)/2})=2$$

のときを除いて，$SL(2,q)$ の既約指標を与えることがわかる．したがって，定理の指標表における $1_G, R, X_m\,(1\leqq m\leqq(q-3)/2)$，$Y_n\,(1\leqq n\leqq(q-1)/2)$ なる既約指標が得られた．ところで，Clifford の定理 8.18 により，$X_{(q-1)/2}, Y_{(q+1)/2}$ は，それぞれ $(q+1)/2$ 次，$(q-1)/2$ 次の既約指標の和に分解される．この分解を求めよう．$X_{(q-1)/2}=\xi_1+\xi_2$ とするとき，Clifford の定理 8.18 により

$$\xi_2(X)=\xi_1(YXY^{-1}), \qquad Y\in GL(2,q)-\langle Z\rangle SL(2,q)$$

である．これから

$$\xi_1(D^i)=\xi_2(D^i), \qquad \xi_1(C^i)=\xi_2(C^i)$$

が得られ，

$$X_{(q-1)/2}(D^i)=2(-1)^i, \qquad X_{(q-1)/2}(C^i)=0$$

より，

$$\xi_1(D^i)=\xi_2(D^i)=(-1)^i, \qquad \xi_1(C^i)=\xi_2(C^i)=0$$

を得る．同様に $Y_{(q+1)/2}=\eta_1+\eta_2$ とするとき

$$\eta_1(D^i)=\eta_2(D^i)=0, \qquad \eta_1(C^i)=\eta_2(C^i)=(-1)^{i+1}$$

を得る．$\xi_i, \eta_i\,(i=1,2)$ の P, P' における値を求めるために，場合を二つに分けよう．

(α) $q\equiv1\pmod 4$ のとき．

$\xi_1(P)=x$，$\xi_1(P')=y$ とおくと，

$$x+y=X_{(q-1)/2}(P)=1$$

である．ところで，$q\equiv1\pmod 4$ であれば，定理 8.32 の (ii) により，$\xi_1(P)=\xi_1(P^{-1})=\overline{\xi_1(P)}$ であるから x, y は実数である．そこで，ξ_1 の内積を計算すると

$$\sum_{X\in SL(2,q)}\xi_1(X)\overline{\xi_1(X)} = \left(\frac{q+1}{2}\right)^2+\left(\frac{q+1}{2}\right)^2+\frac{q^2-1}{2}x^2+\frac{q^2-1}{2}y^2 +\frac{q^2-1}{2}x^2+\frac{q^2-1}{2}y^2+q(q+1)\times\frac{q-3}{2} = q(q^2-1)$$

より

$$x^2+y^2 = \frac{q+1}{2},$$

$$\therefore \quad x = \frac{1\pm\sqrt{q}}{2}, \qquad y = \frac{1\mp\sqrt{q}}{2} \qquad (\text{複号同順})$$

を得る．ここで $\xi_1(P)=\xi_2(P')$, $\xi_1(P')=\xi_2(P)$ に注意すると

$$\xi_1(P) = \xi_2(P') = \frac{1+\sqrt{q}}{2}, \qquad \xi_1(P') = \xi_2(P) = \frac{1-\sqrt{q}}{2}$$

としてよい．同様に η_1, η_2 の P, P' における値を計算することができる．

(β) $q\equiv-1 \pmod 4$ のとき．

$\xi_1(P)=x$ とすると，定理 8.32 の (ii) により $\xi_1(P')=\xi_1(P^{-1})=\overline{\xi_1(P)}=\bar{x}$ である．よって $x+\bar{x}=-1$ である．また ξ_1 の内積を計算して $x\bar{x}=(q+1)/4$ を得る．したがって $x=(-1\pm\sqrt{-q})/2$ となり，$\xi_1(P)=\xi_2(P')=(-1+\sqrt{-q})/2$, $\xi_1(P')=\xi_2(P)=(-1-\sqrt{-q})/2$ としてよいことがわかる．∎

§8.7 指標の応用

この節と次節では，群指標の理論の有限群論への応用を述べる．したがって第7章 (とくに §7.1–§7.3) からの引用がある．取り上げた題材は，現在の有限群論において標準的と思われるものを選んである．この節の a) では，TI 集合とその簡単な性質を述べる．とくに補題 8.17 は，本節および次節において基本的役割を果たす．b) では補題 8.17 の直接の応用として，Frobenius 核の存在を示す古典的な Frobenius の定理 8.34 を証明する．また Frobenius 群の群指標についても述べる (定理 8.35)．c) では，いわゆる例外指標について簡単に説明する．

a) TI 集合

第7章におけるように G の部分集合 S と G の元 x に対して

$$S^x = x^{-1}Sx$$

と書く．さて，有限群 G の部分集合 D が，G の任意の元 x に対して

(8.57)
$$D = D^x \quad \text{または} \quad D \cap D^x \subseteq \{1\}$$

なる条件を満たすとき，D を G の **TI 集合** (trivial intersection set) という．ここで $D\cap D^x \subseteq \{1\}$ は，$D\cap D^x$ が単位元のみから成る集合あるいは空集合 (D が単位元1を含むか含まないかによって起こる区別) であることを意味することに注意する．$H=N_G(D)$ とおくとき，(8.57) は

$$D\cap D^x \subseteq \{1\} \qquad (\forall x \in G-H)$$

と同値である．

補題 8.16　D を G の TI 集合，$H=N_G(D)$ とするとき，

(i)　$D \ni x \neq 1 \Longrightarrow C_G(x) \subseteq H$,

(ii)　D の2元 x, y が G で共役ならば，それらは H ですでに共役である：

$$x \underset{G}{\sim} y \Longrightarrow x \underset{H}{\sim} y.$$

逆に，G の部分群 H と H の部分集合 D で，$D^x=D$ $(\forall x \in H)$ を満たすものが与えられたとき，D が (i), (ii) を満たせば，D は G の TI 集合で $H=N_G(D)$ である．

証明　D を G の TI 集合，$H=N_G(D)$ としよう．

$$g^{-1}xg = y \qquad (g \in G,\ \ x, y \in D)$$

とする．$x=y=1$ ならば，(ii) は明らかに成り立つから $x, y\neq 1$ としよう．このとき，

$$1 \neq y = x^g \subseteq D\cap D^g$$

であるから，(8.57) により $D=D^g$ すなわち $g \in H$ である．(i) は上の議論で $x=y$ とすればよい．逆に $G \supseteq H \supseteq D$, $D=D^h$ $(\forall h \in H)$ としよう．$G-N_G(D) \ni x$ ならば，$D\neq D^x$. $D\cap D^x \ni z=y^x\neq 1$ ならば，(ii) により $z=y^h$ なる $h \in H$ が存在する．このとき $hx^{-1} \in C_G(y)$. (i) により $H \supseteq C_G(y)$ であるから，$H \ni x$ となり矛盾である．よって，$D\cap D^x \subseteq \{1\}$ $(\forall x \in G-N_G(D))$ が成り立つ．とくに $H=N_G(D)$ もわかる．∎

有限群 H の部分集合 D に対して，$H-D$ の上でつねに0であるような H の一般指標の全体を $M_H(D)$ で表わすことにしよう：

$$M_H(D) = \{\varphi \in Cl_Z(H) \mid \varphi(x)=0\ (\forall x \in H-D)\}.$$

つぎの簡単な補題は，本節および次節において極めて重要である．

補題 8.17　D を G の TI 集合，$H=N_G(D)$ とするとき，

(i) $M_H(D) \ni \varphi \Longrightarrow \varphi^G(x)=\varphi(x) \quad (\forall x \in D-\{1\})$,

(ii) $M_H(D) \ni \varphi, \psi,\ \varphi(1)=0 \Longrightarrow (\varphi^G, \psi^G)_G=(\varphi, \psi)_H$.

証明 (i) $D \ni x \neq 1$ とする．(8.41) (§8.4, b)) により，

$$\varphi^G(x)=\frac{1}{|H|}\sum_{y \in G}\varphi^0(y^{-1}xy)$$

である．ところで，

$$\begin{aligned}\varphi^0(y^{-1}xy) \neq 0 &\Longrightarrow y^{-1}xy \in D && (M_H(D) \text{ および } \varphi^0 \text{ の定義})\\ &\Longrightarrow y^{-1}xy \in D \cap D^y \\ &\Longrightarrow D=D^y && (y^{-1}xy \neq 1 \text{ に注意})\\ &\Longrightarrow y \in H\end{aligned}$$

であるから，

$$\varphi^G(x)=\frac{1}{|H|}\sum_{y \in H}\varphi(y^{-1}xy)=\frac{1}{|H|}\sum_{y \in H}\varphi(x)=\varphi(x)$$

を得る．

(ii) Frobenius 相互律(定理 8.17) により，

$$(\varphi^G, \psi^G)=(\varphi^G \mid H, \psi).$$

$\theta=(\varphi^G \mid H)-\varphi$ とおくと，(i) および $\varphi(1)=0$ より，$\theta \in M_H(H-D)$ である．ところで，$M_H(H-D) \subseteqq M_H(D)^{\perp}$ (=内積 $(\ ,\ )_H$ に関する $Cl_Z(H)$ における $M_H(D)$ の直交補空間) であるから，

$$(\varphi^G, \psi^G)=(\varphi^G \mid H, \psi)=(\theta+\varphi, \psi)=(\varphi, \psi)$$

を得る．▌

問 8.26 G の TI 集合 D が，$D^x \cap N_G(D) \subseteqq D \ (\forall x \in G)$ なる条件を満たすとする．$D^G=\bigcup_{x \in G} D^x$ とおくとき，

$$M_H(D) \ni \varphi \longmapsto \varphi^G$$

なる写像は $M_H(D)$ から $M_G(D^G)$ への全単射であることを示せ．

b) Frobenius 群 III

補題 8.17 の最初の応用として，古典的な Frobenius の定理を証明しよう．この定理は，§7.2, e) で述べた Frobenius 群の二つの定義 (i), (ii) (p. 176 参照) のうち (ii) $\Longrightarrow$ (i) を示すものである．逆の (i) $\Longrightarrow$ (ii) はすでに §7.2, e) で述べた．

定理 8.34 (Frobenius) G の真の部分群 H が

(8.58)
$$H \cap H^x = \{1\} \qquad (\forall x \in G-H)$$
を満たすものとする．このとき，
$$G = HN, \qquad H \cap N = \{1\}$$
なる正規部分群 N が存在する．

証明　(8.58) により，H は G の TI 集合で，$H=N_G(H)$ である．θ を H の自明でない既約指標としよう．
$$\xi_\theta = \theta - \theta(1)1_H$$
とおくと，明らかに
$$\xi_\theta(1) = 0, \qquad \xi_\theta \in M_H(H) = Cl_{\boldsymbol{Z}}(H)$$
である．このとき，補題 8.17 の (ii) により

(＊)
$$(\xi_\theta{}^G, \xi_\theta{}^G) = (\xi_\theta, \xi_\theta) = 1+\theta(1)^2$$
を得る．また Frobenius 相互律により

(＊＊)
$$(\xi_\theta{}^G, 1_G) = (\xi_\theta, 1_H) = -\theta(1)$$
である．よって

(＊＊＊)
$$\xi_\theta{}^G = -\theta(1)1_G + \chi_\theta \qquad (\chi_\theta \in Cl_{\boldsymbol{Z}}(G))$$
とおくと，(＊＊) により $(\chi_\theta, \chi_\theta)=1$．また $\xi_\theta{}^G(1)=0$ より $\chi_\theta(1)=\theta(1)>0$ であるから，補題 8.12 により χ_θ は G の既約指標である．
$$G_\theta = \operatorname{Ker} \chi_\theta, \qquad N = \bigcap_\theta G_\theta, \qquad S = G-(H-\{1\})^G$$
とおく．ここで，$\bigcap_\theta G_\theta$ において θ は H のすべての自明でない既約指標を走る．さて，
$$\begin{aligned} |S| &= |G| - |(H-\{1\})^G| \\ &= |G| - \frac{|G|}{|H|}(|H|-1) \qquad ((8.58)\text{による}) \\ &= \frac{|G|}{|H|}, \end{aligned}$$
$$\begin{aligned} S \ni x &\Longrightarrow \xi_\theta{}^G(x) = 0 \\ &\Longrightarrow \chi_\theta(x) = \theta(1) = \chi_\theta(1) \\ &\Longrightarrow x \in G_\theta \end{aligned}$$
であるから

$$(****)\qquad |S|\cdot|H|=|G|,\qquad S\subseteq N$$

を得る．一方，$N\cap H\ni x\neq 1$ とすると，補題 8.17 の (i) によって $\xi_\theta{}^G(x)=\xi_\theta(x)$, $(***)$ により $\xi_\theta{}^G(x)=-\theta(1)+\chi_\theta(x)=-\theta(1)+\chi_\theta(1)=0$ であるから $0=\xi_\theta(x)=\theta(x)-\theta(1)$，すなわち H の自明でないすべての指標 θ に対して $\theta(x)=\theta(1)$ となり，矛盾である．よって

$$N\cap H=\{1\}$$

を得る．これと，$(****)$ より $G=HN$, $H\cap N=\{1\}$ を得る．▌

系 G, H, N を定理 8.34 の通りとするとき，(G, N) は Frobenius 群で H はその Frobenius 補群である．

証明 §7.2, e) における Frobenius 群の定義により

$$N\ni x\neq 1 \Longrightarrow C_G(x)\subseteq N$$

を示せばよい．$C_G(x)\ni y\ (1\neq x\in N)$ としよう．$G=HN$ および (8.58) により，G は N および $H^n\ (n\in N)$ の和集合であるから，$y\notin N$ ならば，$y=h^n\ (h\in H, n\in N)$ と書ける．このとき $z=x^{n^{-1}}$ とおくと，$z\in N$, $z^{-1}hz\in H\cap H^z$．したがって (8.58) により $z\in H$ となり，$H\cap N=\{1\}$ に反する．▌

一般に，有限群が与えられたとき，その正規部分群を見出すことが重要である．上の定理 8.34 は，Frobenius 相互律の応用として，そのような結果を導くもっとも典型的なものである．このほかにも，このような例を後に見るであろう．なお，定理 8.34 は，Brauer の指標定理 8.26 の応用として証明することもできるが，ここでは省略する．——

Frobenius 群の既約指標を調べよう．Frobenius 群の基本的な事柄については §7.2, e) を参照されたい．G を Frobenius 群，N, H をそれぞれ G の Frobenius 核，Frobenius 補群とする．$G/N\simeq H$ であるから，H の既約指標は自然に G の既約指標とみることができる．さて，つぎのことを示そう：

(8.59) N の自明でない既約指標の G への誘導指標は，G の既約指標である．

そのために，つぎの簡単な補題を用いる．これはしばしば利用される便利な補題である．

補題 8.18 (Brauer) G を任意の有限群，A は集合 G に §2.1 の意味で右から作用する有限群でつぎの性質をもつものとする：

(i) K が G の共役類ならば，A の各元 α に対して $K^\alpha=\{k^\alpha \mid k\in K\}$ も G の

共役類である.

(ii) χ が G の既約指標のとき, $\chi^\alpha(x)=\chi(x^\alpha)$ とおけば, χ^α も G の既約指標である.

このとき, A の各元 α に対して, $K^\alpha=K$ なる共役類の数と $\chi^\alpha=\chi$ なる G の既約指標の数は同じである.

証明 $K_1, K_2, \cdots, K_h$ を G の共役類の全体, $\chi_1, \chi_2, \cdots, \chi_h$ を G の既約指標の全体とする. $K_j \ni x_j$ とするとき,

$$X=(\chi_i(x_j))$$

なる h 次行列 X を考える. 直交関係により X は正則行列である. また, (i), (ii) により A の各元は, X の行および列の置換をひき起こす:

$$X^\alpha=(\chi_i{}^\alpha(x_j))=(\chi_i(x_j{}^\alpha)) \qquad (\alpha \in A).$$

したがって, 置換行列 $P(\alpha), Q(\alpha)$ が存在して

$$X^\alpha=P(\alpha)X=XQ(\alpha) \quad \text{とくに} \quad P(\alpha)=XQ(\alpha)X^{-1}$$

である. また $(X^\alpha)^\beta=X^{\alpha\beta}$ より

$$P(\alpha\beta)=P(\alpha)P(\beta), \qquad Q(\alpha\beta)=Q(\beta)Q(\alpha) \qquad (\alpha, \beta \in A)$$

であるから, $\alpha \mapsto P(\alpha)$, $\alpha \mapsto {}^tQ(\alpha)$ なる A の置換表現を得る. それぞれの指標を θ_1, θ_2 とするとき,

$$\begin{aligned}\theta_1(\alpha)&=\mathrm{tr}\,(P(\alpha))=\mathrm{tr}\,(XQ(\alpha)X^{-1})\\&=\mathrm{tr}\,(Q(\alpha))=\mathrm{tr}\,({}^tQ(\alpha))=\theta_2(\alpha)\end{aligned}$$

であるから, 例8.8により補題8.18の結論が得られる. ▌

Frobenius 群に戻る. H の N への作用

$$x^h=h^{-1}xh \qquad (h \in H,\ x \in N)$$

を考える. この作用は補題8.18の (i), (ii) を満たすことに注意する. さらに N の共役類 $K \neq \{1\}$ をとると, $K^h \neq K$ $(1 \neq \forall h \in H)$ である. 実際, $K^h=K$ とすると, $x^h=y$ $(x, y \in K)$ であるが, $x^n=y$ なる N の元 n が存在するから, $x^{hn^{-1}}=x$. よって $hn^{-1} \in C_G(x) \subseteqq N$. このとき, $1 \neq h \in H \cap N$ となり矛盾である. したがって, 補題8.18により, H の元 $h \neq 1$ で固定される N の既約指標は自明なものに限る:

$$\theta^h \neq \theta \qquad (1 \neq h \in H,\ \theta \in \mathrm{Irr}\,(N)-\{1_N\}). \tag{8.60}$$

さて,

(8.61) $\mathrm{Irr}(N)\ni\theta\mapsto\theta^G$ なる対応は，$\mathrm{Irr}(N)-\{1_N\}$ から $\{\chi\in\mathrm{Irr}(G)\mid\mathrm{Ker}\,\chi \not\supseteq N\}$ への全射

である．実際，$\mathrm{Irr}(N)\ni\theta\neq 1_N$ とすると，(8.60) により θ の G に関する惰性群は N に一致する．したがって定理 8.19 により，θ^G は G の既約指標である．$\theta\neq 1_N$ より $\mathrm{Ker}\,\theta^G\not\supseteq N$ である．逆に χ を $\mathrm{Ker}\,\chi\not\supseteq N$ なる G の既約指標とするとき，θ を $\chi|N$ の既約成分とすれば，Clifford の定理 8.18 により $\theta\neq 1_N$ であり，したがって $\theta^G\in\mathrm{Irr}(G)$ すなわち $\theta^G=\chi$ を得る．これで (8.61) が示された．

$\mathrm{Irr}(N)-\{1_N\}\ni\theta_1,\theta_2$ とすると，Frobenius 相互律により θ_i は $\theta_i{}^G|N$ の既約成分であるから，$\theta_1{}^G=\theta_2{}^G$ ならば，θ_1 と θ_2 は G で共役である．このとき $G=HN$ より，$\theta_1{}^h=\theta_2$ $(\exists h\in H)$ である．このことと，(8.60), (8.61) から，$\mathrm{Ker}\,\chi\not\supseteq N$ なる G の既約指標の数は，N の共役類の数を $h(N)$ とするとき，$(h(N)-1)/|H|$ であることがわかる．以上まとめてつぎの定理を得る．

定理 8.35 G を Frobenius 群，N, H をそれぞれ G の Frobenius 核，Frobenius 補群とする．また，H, N の共役類の数を $h(H), h(N)$ とするとき，つぎの (i), (ii) が成り立つ：

(i) G は N を核に含む $h(H)$ 個の既約指標をもつ．これらは，H の既約指標 (を G の既約指標とみたもの) にほかならない．

(ii) N の自明でない既約指標の G への誘導指標は，N を核に含まない G の既約指標である．また，N を核に含まない G の既約指標はすべてこのようにして得られ，$(h(N)-1)/|H|$ 個存在する．

c) 例外指標

補題 8.19 (Brauer-Suzuki) D を G の TI 集合，$H=N_G(D)$ とする．$\xi_1, \xi_2, \cdots, \xi_w$ は H の異なる既約指標でつぎの性質をもつものとする：

(i) $\xi_1(1)=\xi_2(1)=\cdots=\xi_w(1)$,

(ii) $\xi_i-\xi_j\in M_H(D)$ $(1\leqq i, j\leqq w)$.

$w\geqq 2$ ならば，G の既約指標 $\chi_1, \chi_2, \cdots, \chi_w$ と符号 ε が存在して，

$$(\xi_i-\xi_j)^G=\varepsilon(\chi_i-\chi_j)\qquad(1\leqq i, j\leqq w)$$

となる．

証明 まず $w=2$ とする．補題 8.17 により

$$((\xi_1-\xi_2)^G, (\xi_1-\xi_2)^G)=(\xi_1-\xi_2, \xi_1-\xi_2)=2$$

であるから，$(\xi_1-\xi_2)^G \in Cl_Z(G)$，$\xi_1{}^G(1)=\xi_2{}^G(1)$ に注意すれば，

$$(\xi_1-\xi_2)^G = \chi_1-\chi_2$$

なる G の既約指標 χ_1, χ_2 が存在する．よって $w=2$ のとき $\varepsilon=1$ とすれば補題が成り立つ．$w \geqq 3$ としよう．まず

$$(\xi_1-\xi_2)^G = \chi_1-\chi_2$$

なる $\chi_1, \chi_2 \in \mathrm{Irr}(G)$ を上と同様にしてとることができる．このとき，補題8.17により

$$((\xi_1-\xi_2)^G, (\xi_1-\xi_3)^G) = (\xi_1-\xi_2, \xi_1-\xi_3) = 1$$

であるから，

$$(\xi_1-\xi_3)^G = \chi_1-\chi_3 \quad \text{または} \quad \chi_3-\chi_2$$

なる $\chi_3 \in \mathrm{Irr}(G)$ が存在する．ここで，場合を二つに分けよう．

(α)　$(\xi_1-\xi_3)^G=\chi_1-\chi_3$ の場合．

$j>3$ に対して

$$((\xi_1-\xi_2)^G, (\xi_1-\xi_j)^G) = (\xi_1-\xi_2, \xi_1-\xi_j) = 1,$$
$$((\xi_1-\xi_3)^G, (\xi_1-\xi_j)^G) = (\xi_1-\xi_3, \xi_1-\xi_j) = 1$$

より，$(\xi_1-\xi_j)^G=\chi_1-\chi_j$ ($\chi_j \in \mathrm{Irr}(G)$) の形でなければならない．このとき，$\varepsilon=1$ として補題が成り立つ．

(β)　$(\xi_1-\xi_3)^G=\chi_3-\chi_2$ の場合．

$\varepsilon=-1$，$\chi_2=\zeta_1$，$\chi_1=\zeta_2$，$\chi_3=\zeta_3$ とおくと

$$(\xi_1-\xi_2)^G = \varepsilon(\zeta_1-\zeta_2), \qquad (\xi_1-\xi_3)^G = \varepsilon(\zeta_1-\zeta_3)$$

である．このとき，(α)の場合と同様にして

$$(\xi_1-\xi_j)^G = \varepsilon(\zeta_1-\zeta_j) \qquad (j>3)$$

でなければならないことがわかる．▮

上の補題8.19で現われた G の既約指標 $\chi_1, \chi_2, \cdots, \chi_w$ を $\xi_1, \xi_2, \cdots, \xi_w$ に対応する**例外指標**という．この例外指標の概念は，その一般化とともに1950年以降の有限群論に極めて有効に応用され，多くの成果をあげてきている．その主なものをあげても，Zassenhaus 群の分類，Feit-Thompson による奇数位数の群の可解性の証明などがある．本書では，例外指標の一般化にふれる余裕がないので，以下上で定義した例外指標が応用されるもっとも簡単な場合を説明しておこう．

A が G の可換部分群で

$$(8.62) \qquad A \ni a \neq 1 \implies C_G(a) = A$$

なる条件を満たすものとする．このとき A は G の TI 集合である．実際，$A \cap A^x \ni a = b^x \neq 1$ $(a, b \in A)$ とすると，$A = C_G(a) = C_G(b^x) = C_G(b)^x = A^x$ となり，A は (8.57) を満たす．以下，

$$A^\sharp = A - \{1\},$$
$$H = N_G(A) = N_G(A^\sharp),$$
$$n = |A|,$$
$$l = [H : A],$$
$$w = \frac{n-1}{l}$$

とおく．ここで $l>1$ ならば，H は A を Frobenius 核とする Frobenius 群であることに注意する．したがって，w は整数である．また定理 8.35 から，つぎのことが直ちに得られる：

H の既約指標は，H/A の既約指標と，A を核に含まない w 個の既約指標からなる[1].

ξ_0 を H/A の正則表現の指標，$\xi_1, \xi_2, \cdots, \xi_w$ を A を核に含まない H の既約指標とする．ξ_i $(i>0)$ は A の既約指標の誘導指標であるから

$$\xi_1(1) = \xi_2(1) = \cdots = \xi_w(1),$$
$$\xi_i \in M_H(A) \qquad (i=1, 2, \cdots, w)$$

となり，補題 8.19 の条件を満たすことに注意する．

補題 8.20 (Brauer-Suzuki)　$G, A, H, \xi_0, \xi_1, \cdots, \xi_w$ は上の通りとして，$w \geqq 2$ と仮定する．$\chi_1, \chi_2, \cdots, \chi_w$ を $\xi_1, \xi_2, \cdots, \xi_w$ に対応する例外指標，ε をその符号とするとき，つぎの (i)-(iv) が成り立つ：

(i)　$\xi_0{}^G = 1_G + \alpha \sum_{i=1}^{w} \chi_i + \Delta_0 \quad (\alpha \in \boldsymbol{Z}),$

$\xi_i{}^G = \varepsilon\chi_i + \beta \sum_{i=1}^{w} \chi_i + \Delta \quad (\beta \in \boldsymbol{Z}).$

ここで，Δ_0, Δ は自明でない非例外指標の整係数 1 次結合で，Δ は i によらない．

(ii)　$A^\sharp \ni \sigma$ に対して，$\chi_i(\sigma) = \varepsilon\xi_i(\sigma) + \alpha - \beta$．$\Delta_0 = \sum_j a_j\zeta_j$，$\Delta = \sum_j b_j\zeta_j$ $(\zeta_j \in$

---

1) $l=1$ でもよいことに注意.

$\mathrm{Irr}(G)-\{\chi_1, \chi_2, \cdots, \chi_w\}$) とするとき，$\zeta_j(\sigma)=a_j-b_j$ ($\sigma\in A^\sharp$)．すなわち，$\xi_k{}^G$ ($0\leqq k\leqq w$) の既約指標への分解がわかると，G の各既約指標の $A^\sharp$ の上での値がわかる．

(iii) $l=(\alpha-\beta)^2(w-1)+(\alpha-\beta-\varepsilon)^2+\sum_j(a_j-b_j)^2$.

(iv) $\zeta_j(1)\equiv a_j-b_j \pmod n$, $\quad (a_j-b_j)^2\leqq \dfrac{n-1}{2}$.

証明　(i)

$$\begin{aligned}(\xi_0{}^G, 1_G) &= (\xi_0, 1_H) = 1 \qquad (\text{Frobenius 相互律}),\\ (\xi_0{}^G, \chi_i-\chi_j) &= \varepsilon(\xi_0{}^G, (\xi_i-\xi_j)^G)\\ &= \varepsilon(\xi_0, \xi_i-\xi_j) \qquad (\text{補題 8.17})\\ &= 0\end{aligned}$$

であるから，$\xi_0{}^G=1_G+\alpha\sum_{i=1}^{w}\chi_i+\Delta_0$，$(\Delta_0, 1_G)=(\Delta_0, \chi_i)=0$ なる分解が得られる．また，$i>0$ に対して

$$\begin{aligned}(\xi_i{}^G, 1_G) &= (\xi_i, 1_H) = 0,\\ (\xi_i{}^G, \chi_i-\chi_j) &= \varepsilon(\xi_i{}^G, (\xi_i-\xi_j)^G)\\ &= \varepsilon(\xi_i, \xi_i-\xi_j)\\ &= \varepsilon\end{aligned}$$

より，$(\xi_i{}^G, \chi_i)=\varepsilon+(\xi_i{}^G, \chi_j)$ $(i\neq j)$ であるから，

$$\xi_i{}^G = \varepsilon\chi_i+\beta_i\sum_{j=1}^{w}\chi_j+\Delta_i, \qquad (\Delta_i, 1_G) = (\Delta_i, \chi_j) = 0$$

なる分解が得られる．β_i, Δ_i が i によらないことは，$(\xi_i-\xi_j)^G=\varepsilon(\chi_i-\chi_j)$ からわかる．

(ii) Frobenius 相互律と (i) から，

$$\chi_i\,|\,H = \varepsilon\xi_i+\beta\sum_{j=1}^{w}\xi_j+\Phi_i, \qquad (\Phi_i, \xi_j) = 0 \quad (1\leqq j\leqq w)$$

である．よって

$$\chi_i(\sigma) = \varepsilon\xi_i(\sigma)+\beta\sum_{j=1}^{w}\xi_j(\sigma)+\Phi_i(\sigma) \qquad (\sigma\in A^\sharp).$$

ところで，$1+\sum_{j=1}^{w}\xi_j(\sigma)$ は A のすべての既約指標の σ における値の和であるから，

$$1+\sum_{j=1}^{w}\xi_j(\sigma) = 0, \qquad \therefore\quad \sum_{j=1}^{w}\xi_j(\sigma) = -1.$$

一方,

$$\alpha = (\xi_0{}^G, \chi_i) = (\xi_0, \chi_i \mid H)$$
$$= (\xi_0, \varepsilon\xi_i + \beta \sum \xi_j + \Phi_i)$$
$$= (\xi_0, \Phi_i).$$

$(\Phi_i, \xi_j)=0$ より Φ_i は A を核に含む H の指標であり, ξ_0 は H/A の正則表現の指標であるから,

$$\xi_0 = \sum_k \varphi_k(1)\varphi_k, \qquad \Phi_i = \sum_k a_{ik}\varphi_k, \qquad \varphi_k \in \mathrm{Irr}\,(H/A)$$

とすると,

$$\alpha = (\xi_0, \Phi_i) = \sum_k a_{ik}\varphi_k(1) = \Phi_i(1) = \Phi_i(\sigma) \qquad (\sigma \in A)$$

を得る. したがって

$$\chi_i(\sigma) = \varepsilon\xi_i(\sigma) + \alpha - \beta \qquad (\sigma \in A^{\sharp})$$

である. まったく同様にして

$$\zeta_j(\sigma) = a_j - b_j \qquad (\sigma \in A^{\sharp})$$

を得る.

(iii) 補題 8.17 により

$$((\xi_0 - \xi_i)^G, (\xi_0 - \xi_i)^G) = (\xi_0 - \xi_i, \xi_0 - \xi_i) = l+1$$

であるから,

$$\xi_0{}^G - \xi_i{}^G = 1_G - \varepsilon\chi_i + (\alpha - \beta)\sum_{j=1}^{w}\chi_j + \sum_j (a_j - b_j)\zeta_j$$

の両辺の内積を比べて (iii) を得る.

(iv) $\sum_{\sigma \in A} \zeta_j(\sigma) \equiv 0 \pmod n$ であるから, (ii) により

$$\zeta_j(1) + (n-1)(a_j - b_j) \equiv 0 \pmod n,$$
$$\therefore \quad \zeta_j(1) \equiv a_j - b_j \pmod n$$

を得る. また (iii) により

$$(a_j - b_j)^2 \leqq l \leqq \frac{n-1}{2}$$

である. ▌

G の可換部分群 A が, (8.62), $w=(n-1)/l \geqq 2$ を満たすとき, 補題 8.20 における G の w 個の既約指標 $\chi_1, \chi_2, \cdots, \chi_w$ を A **に対する例外指標**ということに

しよう．A_1, A_2 がともに上の条件を満たし，A_1 と A_2 が G で共役でないならば，補題8.20の(ii)により A_i に対する G の例外指標は，A_j $(j \neq i)$ に対しては例外指標ではない．

例8.19　G, A は(8.62)を満たし，

$$l=2, \quad w=\frac{n-1}{2} \geqq 2$$

とする．このとき，$((\xi_0-\xi_i)^G, (\xi_0-\xi_i)^G)=3$ であるから，

$$\xi_0{}^G-\xi_i{}^G = 1_G+\varepsilon\Phi-\varepsilon\chi_i, \qquad (\Phi, \chi_i) = 0$$

なる分解をもち，Φ は A に対して非例外指標である．Ψ を A に対する非例外指標で Φ と異なるものとして，$\sigma \in A^\sharp$，τ を A の元と共役でない G の元，$\Phi(1)=f$，$\Phi(2)=x$ とおくと，補題8.20から指標表についてつぎのことがわかる：

	1	τ	σ
1_G	1	1	1
χ_i	$f+\varepsilon$	$x+\varepsilon$	$\varepsilon\xi_i(\sigma)$
Φ	f	x	ε
Ψ	$*$	$*$	0

5次交代群 $\mathfrak{A}_5$ の位数5の部分群 A は，この例の条件 $l=2$ を満たす．A に対応する2個の例外指標は，例8.14における3次指標，Φ は4次指標である．上に述べたこの例の結果と例8.14における計算を比べられたい．

例8.20　$G=SL(2, 2^n)$ $(n \geqq 3)$ とする．$q=2^n \geqq 8$ とおくと $|G|=q(q^2-1)$ である．G は位数 $q-1$ の元 δ と位数 $q+1$ の元 γ をもち，

$$A_{-1} = \langle\delta\rangle, \qquad A_1 = \langle\gamma\rangle$$

とおくと，A_{-1}, A_1 はともに(8.62)を満たし，

$$[N_G(A_{-1}) : A_{-1}] = [N_G(A_1) : A_1] = 2$$

である．また，τ を G の位数2の元とするとき，

$$1, \quad \tau, \quad \delta^s \left(1 \leqq s \leqq \frac{q-2}{2}\right), \quad \gamma^t \left(1 \leqq t \leqq \frac{q}{2}\right)$$

が，G の共役類の代表元である．さて，$\chi_1, \chi_2, \cdots, \chi_{(q-2)/2}$ を A_{-1} に対する例外指標，$\chi_1', \chi_2', \cdots, \chi_{q/2}'$ を A_1 に対する例外指標とするとき，例8.19における Φ は，$\{\chi_i\}, \{\chi_j'\}$ に対して共通であって G の指標表はつぎの形になる：

	1	τ	δ^s	γ^t	
1_G	1	1	1	1	
Φ	f	x	ε	ε'	
χ_i	$f+\varepsilon$	$x+\varepsilon$	$*$	0	$\left(1\leqq i\leqq\dfrac{q-2}{2}\right)$
χ_j'	$f+\varepsilon'$	$x+\varepsilon'$	0	$*$	$\left(1\leqq j\leqq\dfrac{q}{2}\right)$.

最後の二つの列の直交関係から $1+\varepsilon\varepsilon'=0$，よって $\varepsilon'=-\varepsilon$ を得る．第1列の直交関係から，

$$1+f^2+\frac{q-2}{2}(f+\varepsilon)^2+\frac{q}{2}(f-\varepsilon)^2 = q(q^2-1),$$

$$\therefore\quad f = q,\qquad \varepsilon = 1$$

である．第1列と第2列の直交関係から $x=0$ である．最後に $\chi_i(\delta^s)$，$\chi_j'(\gamma^t)$ の値は補題 8.20 の (ii) から得られ，$G=SL(2,2^n)$ の指標表が完成する．

例題 8.3 (Suzuki)　G をつぎの条件を満たす有限群とする：

(8.63) $$G\ni x\neq 1 \Longrightarrow C_G(x)\text{ は可換部分群.}$$

このとき，G の位数が奇数ならば G は可解群である．

注意　この例題は，奇数位数の群の可解性に関する Feit–Thompson の定理の非常に特別な場合である．したがって現在では，この命題自体に特別の意味があるわけではないが，鈴木通夫氏によるこの命題の証明が，Feit–Thompson による一般の場合の証明の方向を暗示するものであったという歴史的意義を忘れてはならない．その意味で以下の証明が読者の興味をひき起こすことを期待する．もちろん，Feit–Thompson の証明の複雑さは，以下の証明の比ではなく，Feit–Thompson の両天才が必要であったことは確かなことである．

[証明]　G の互いに共役でない極大可換部分群の全体を

$$A_1,\quad A_2,\quad \cdots,\quad A_s$$

とする．(8.63) から，各 A_i は (8.62) を満たし，A_i は TI 集合，さらに $A_i\cap A_j=1$ $(i\neq j)$ である．また G の各元は或る A_i の元に共役である．したがって，

$$n_i = |A_i|,\qquad l_i = [N_G(A_i):A_i],\qquad w_i = \frac{n_i-1}{l_i}$$

とおくと，G の類等式は

(8.64) $$|G| = 1+\sum_{i=1}^{s}\frac{|G|}{n_i}w_i$$

となる(補題8.16参照)．また，G は $1+\sum_{i=1}^{s} w_i$ 個の共役類をもつことがわかる．また G は奇数位数の群であるから，$w_i=(n_i-1)/l_i$ は偶数となり，とくに

$$w_i \geqq 2 \qquad (i=1, 2, \cdots, s)$$

である．したがって，各 i の A_i に対する w_i 個の例外指標

$$\Theta_j^{\,i} \qquad (j=1, 2, \cdots, w_i)$$

が存在する．これらは，すべて異なる G の既約指標であるから，恒等指標と $\Theta_j^{\,i}$ $(1\leqq i\leqq s,\ 1\leqq j\leqq w_i)$ が G のすべての既約指標を与えることがわかる．

さて，必要ならば番号をつけ変えて $n_s\leqq n_i$ $(i=1, 2, \cdots, s)$ としてよい．そこで，

$$n = n_s, \qquad l = l_s, \qquad w = w_s, \qquad d = \Theta_i^{\,s}(1)$$

とおき，さらに

$$1 \leqq i \leqq t \quad \text{のとき} \quad n_i \,|\, d,$$
$$t < i \leqq s \quad \text{のとき} \quad n_i \nmid d$$

なるように $n_1, n_2, \cdots, n_s$ を並べる．$\Theta=\Theta_1^{\,s}$ とおくと，第1直交関係により

$$|G| = d^2+\sum_{i=1}^{s}\frac{|G|}{n_i l_i}\sum_{\sigma\in A_i^{\#}}|\Theta(\sigma)|^2 \tag{8.65}$$

である．ここで

$$1 \leqq i \leqq t \qquad \text{のとき} \quad \sum_{\sigma\in A_i^{\#}}|\Theta(\sigma)|^2 = 0,$$
$$t < i \leqq s-1 \quad \text{のとき} \quad \sum_{\sigma\in A_i^{\#}}|\Theta(\sigma)|^2 \geqq n_i-1 = w_i l_i,$$
$$i = s \qquad \text{のとき} \quad \sum_{\sigma\in A_s^{\#}}|\Theta(\sigma)|^2 \geqq l(n-l)$$

を示そう．$i<s$ のとき，Θ は A_i に対して非例外指標である．$1\leqq i\leqq t$ ならば，$n_i\,|\,d$ であるから A_i に対する例外指標に補題8.20の(ii),(iv)を適用して，$\Theta(\sigma)=0$ $(\sigma\in A_i^{\#})$ となり，上の第1式が得られる．$t<i\leqq s-1$ ならば，同様に補題8.20の(ii),(iv)により，$\Theta(\sigma)$ は0でない整数となり，上の第2式を得る．最後に $i=s$ としよう．このとき A_s に対する例外指標に補題8.20の(ii)を適用すれば，$\Theta(\sigma)=\varepsilon\xi_1(\sigma)+a$ $(\sigma\in A_s^{\#},\ a\in \boldsymbol{Z})$ であるから，

$$\begin{aligned}\sum_{\sigma\in A_s^{\#}}|\Theta(\sigma)|^2 &= \sum_{\sigma\in A_s^{\#}}(\varepsilon\xi_1(\sigma)+a)(\varepsilon\overline{\xi_1(\sigma)}+a)\\ &= \sum_{\sigma\in A_s^{\#}}|\xi_1(\sigma)|^2+a\varepsilon\sum_{\sigma\in A_s^{\#}}(\xi_1(\sigma)+\overline{\xi_1(\sigma)})+a^2(n-1)\end{aligned}$$

である．ξ_1 は $N_G(A_s)$ の既約指標で $\xi_1(1)=l$，$\xi_1(x)=0$ $(x\in N_G(A_s)-A_s)$ に注

意すると,

$$= nl-l^2-2a\varepsilon l+a^2(n-1)$$
$$\geqq nl-l^2+l(wa-2a\varepsilon)$$
$$\geqq nl-l^2 \qquad (w\geqq 2 \text{ に注意}).$$

すなわち上の第3式を得る．したがって，(8.65)より

$$|G| \geqq d^2+\sum_{i=t+1}^{s-1}\frac{|G|}{n_i}w_i+\frac{|G|(n-l)}{n}$$

を得る．これと(8.64)から,

$$1+\sum_{i=1}^{t}\frac{|G|}{n_i}w_i+\frac{|G|}{n}w \geqq d^2+\frac{|G|(n-l)}{n}$$

であるが，$n\leqq n_i$ に注意して

(8.66) $$\frac{1}{n}\sum_{i=1}^{t}w_i+\frac{l+w}{n} \geqq 1+\frac{d^2-1}{|G|}$$

を得る．ここで

(8.67) $$l-1 \geqq \sum_{i=1}^{t}w_i$$

を示そう．A_s, $\Theta_1{}^s=\Theta$ に補題8.20の(i)を適用すると,

$$\xi_0{}^G-\xi_1{}^G = 1_G-\varepsilon\Theta+a\sum_{j=1}^{w_s}\Theta_j{}^s+\sum_{i\neq s}b_{ij}\Theta_j{}^i \qquad (a, b_{ij}\in \boldsymbol{Z})$$

なる形の分解が得られるが，$\Theta_1{}^i, \Theta_2{}^i, \cdots, \Theta_{w_i}{}^i$ の次数は等しいから，補題8.20の(ii),(iv)により $b_{i1}=b_{i2}=\cdots=b_{iw_i}$ となり，上の分解は,

(8.68) $$\xi_0{}^G-\xi_1{}^G = 1_G-\varepsilon\Theta+a\sum_{j=1}^{w_s}\Theta_j{}^s+\sum_{i\neq s}b_i\sum_{j=1}^{w_i}\Theta_j{}^i$$

の形となり，補題8.20の(iii)により

(8.69) $$l+1 = 1+(a-\varepsilon)^2+a^2(w-1)+\sum_{i\neq s}b_i{}^2w_i$$

である．ところで，$1\leqq i\leqq t$ のとき $b_i\neq 0$ である．実際，$1\leqq i\leqq t$, $A_i\ni\sigma$ とすると,

$(\xi_0{}^G-\xi_1{}^G)(\sigma) = 0$,

$\Theta_j{}^s(\sigma) = 0$ (補題8.20の(ii),(iv)を A_i に対して適用),

$\Theta_j{}^\mu(\sigma) \in \boldsymbol{Z}$ $(\mu\neq i)$ (上と同様)

であるから，$b_i=0$ とすると，(8.68)から

$$0=1+\sum_{\mu\neq i}b_\mu w_\mu \Theta_j{}^\mu(\sigma), \qquad \Theta_j{}^\mu(\sigma)\in \boldsymbol{Z}$$

となり，右辺は奇数であるから矛盾である．したがって(8.69)から，

$$l+1\geqq 1+1+\sum_{i=1}^{t}b_i^2 w_i \geqq 2+\sum_{i=1}^{t}w_i.$$

すなわち(8.67)を得る．このとき，(8.66), (8.67)から

$$\frac{l-1}{n}+\frac{l+w}{n}\geqq 1+\frac{d^2-1}{|G|}.$$

ここで $d\neq 1$ とすると，

$$l-1+l+w>lw+1,$$
$$\therefore\quad (l-1)(2-w)>0$$

となり，$l\geqq 1$, $w\geqq 2$ に反する．したがって $d=1$ である．これは，G の交換子群 G' が G と異なることを意味する：$G\neq G'$．ところで明らかに G' も(8.63)を満たすから，G' は可解群としてよい．したがって G も可解群でなければならない．▌

問 8.27 G を(8.63)を満たす可解群とするとき，G は Abel 群か Frobenius 群であることを示せ．［ヒント］G の Fitting 部分群に注目．なお，(8.63)を満たす非可解群は $SL(2,2^n)$ $(n\geqq 2)$ に限ることが知られている．

§8.8 偶数位数の群

偶数位数の群は，位数2の元を含む(定理2.2)．位数2の元は，奇素数位数の元に類似を見出すことのできない取り扱いが可能で，それが偶数位数の群を調べる上に有力な手段を提供する．とくに Feit–Thompson の定理により，非可換単純群は偶数位数であるから，位数2の元は有限単純群論において重要となる．a)では，位数2の元の取り扱い方を簡単な例題によって示す．また Brauer–Fowler の定理8.36–8.37を証明する．ただしその証明は，通常のものとは異なり，Frobenius–Schur の定理8.25に基づく群指標を利用するものを述べる．b)では4元数型の Sylow 2部分群をもつ群の非単純性に関する Brauer–Suzuki の定理を証明する．最後にc)では，正2面体群を Sylow 2部分群とする有限群の分類において基本的な Brauer–Suzuki–Wall の定理について述べる．b), c)における群指標の応用は，簡単な補題8.17に基づくものであることに注意されたい．

a) 位数2の元

以下，つぎの記号を用いる．

$|x| = x$ の位数,

$I(G) = \{x \in G \mid |x|=2\}$,

$i(G) =$ 位数 2 の元からなる G の共役類の数,

$\mathrm{Syl}_p(G) = G$ の Sylow p 部分群全体の集合.

また, (2, 2) 型の基本 Abel 群を **4 元群** (four group) という (4 元群と 4 元数群あるいは 4 元数型の群とを混同しないように注意).

定理 2.2 により,

$$|G| = \text{偶数} \iff I(G) \neq \phi$$

である. さて, 位数 2 の元のもっとも大切な性質はつぎの簡単な事実にある:

(8.70) $\quad I(G) \ni u, v, \quad x = uv$ とすると $\quad x^u = x^v = x^{-1}$.

実際, $x^u = u^{-1}xu = u^{-1}(uv)u = vu = (uv)^{-1}$ ($u = u^{-1}$, $v = v^{-1}$ に注意). 同様に $x^v = x^{-1}$ である.

一般に, $G \ni x, y$, $x^y = x^{-1}$ のとき, y は x を**逆転する**ということにしよう. 明らかに

(8.71) $\quad I(G) \ni u$, $G \ni x$ とするとき

$$I(G) \ni ux \iff u \text{ は } x \text{ を逆転する}.$$

これから, H を G の部分群, $I(G) \ni u$ とするとき

(8.72) $\quad |Hu \cap I(G)| = u$ によって逆転される H の元の数

であることがわかる. また, 補題 7.18 により

(8.73) 位数 2 の元 t が奇数位数の群 X に固定点なしに作用するとき, X は Abel 群で, t は X の各元を逆転する

ことに注意する. つぎの補題はこのことの補足である.

補題 8.21 位数 2 の元 t が, 偶数位数の群 X に作用しているとき, t は X の或る位数 2 の元を固定する.

証明 半直積 $\langle t \rangle X$ を作り, t を含む $\langle t \rangle X$ の Sylow 2 部分群を S とする. X は偶数位数だから $S \cap X \neq 1$, $S \cap X \lhd S$ より $(S \cap X) \cap Z(S) \neq 1$. よって, y を $(S \cap X) \cap Z(S)$ の位数 2 の元とすると, $y^t = y$ である. ▌

例題 8.4 G をつぎの性質をもつ有限単純群とする:

$(*) \qquad C_G(t) = 4$ 元群 $\qquad (\forall t \in I(G))$.

このとき, G は 5 次交代群 $\mathfrak{A}_5$ と同型である.

[証明]　$\mathrm{Syl}_2(G) \ni S$ とすると，$C_G(t)=S$ $(\forall t \in S-\{1\})$ である．実際 $I(Z(S)) \ni t$ とすると $S \subseteqq C_G(t)$ であるが，(＊)により $C_G(t)$ は2群であるから，$S=C_G(t)$ でなければならない．とくに

$$C_G(S) = S, \qquad S = 4\ \text{元群}$$

である．$N=N_G(S)$ とおくと，4元群の自己同型群を考えて $|N/S|=1$ または3であるが，G の単純性と Burnside の定理7.14により，$|N/S|=3$ でなければならない．このとき，$N \simeq \mathfrak{A}_4$ (=4次交代群) である．とくに G の位数2の元はすべて共役である．よって $|I(G)|=|G|/4$ であることがわかる．また G の単純性により $G \neq N$ であり，さらに Sylow の定理により

$$G-N \ni x \Longrightarrow N \neq N^x$$

であることに注意する(補題5.7，p.124参照)．さて，

(＊＊)　$N \neq Nx$　ならば　Nx はちょうど3個の位数2の元を含む

ことを示そう．$I(G) \cap Nx \ni u$ とすると，u は $N \cap N^u$ に作用するが，$C_G(t)=S$ $(\forall t \in S-\{1\})$ と補題8.21により $|N \cap N^u|$ は奇数，よって $|N \cap N^u| \leqq 3$ である．u によって逆転される N の元は $N \cap N^u$ に含まれるから，(8.72)により $Nx=Nu$ に含まれる位数2の元の数は高々3である．したがって

$$\begin{aligned} \frac{|G|}{4} = |I(G)| &\leqq |N \cap I(G)| + 3\left(\frac{|G|}{|N|}-1\right) \\ &= 3+\frac{|G|}{4}-3 = \frac{|G|}{4} \end{aligned}$$

であるから，上の不等号は等号となり(＊＊)がわかる．さらに上の推論から，

(＊＊＊)　$I(G)-N \ni u \Longrightarrow |N \cap N^u|=3$ で，u は $N \cap N^u$ の各元を逆転する

ことがわかる．T を N の位数3の部分群としよう．$G-N \ni x$，$T^x=T$ とすると，(＊＊)により $Nx=Nu$ $(\exists u \in I(G))$ であるから，$xu \in N$．また，$T=T^x=N \cap N^x = N \cap N^u$ より $T^u=T$．よって $xu \in N_N(T)=T$．$T=N \cap N^u$ であるから，(＊＊＊)により $x \in Tu \subseteqq I(G)$ で x は T の各元を逆転する．これは，$C_G(T)=T$，$|N_G(T)|=6$ を示し，とくに T の各元を逆転する G の位数2の元は，ちょうど3個あることがわかる．N は位数3の部分群を4個もつから，(＊＊＊)により

$$\frac{|G|}{4} = |I(G)| = |N \cap I(G)| + 3\times 4 = 3+12 = 15,$$

$$\therefore \quad |G| = 60$$

を得る．G の G/N での置換表現を考えると，G の単純性より，この置換表現は忠実であり，$|G/N|=5$ より $G\simeq\mathfrak{A}_5$ がわかる．▌

類似の例題をもう一つあげよう．

例題 8.5 G をつぎの性質をもつ有限群とする：

(i) G の位数 2 の元はすべて共役，

(ii) $C_G(t) = D_8$ (位数 8 の正 2 面体群) $(\forall t \in I(G))$.

このとき，$|G|=168$ または 360 である．

注意 実際は，$G\simeq PSL(2,7)$ あるいは $PSL(2,9)$ である (§8.8, c) の Brauer-Suzuki -Wall の定理とそれに続く説明を参照)．

[証明] (Bender) (i), (ii) により G の Sylow 2 部分群は位数 8 の正 2 面体群である．V を G の 4 元部分群とし，$N=N_G(V)$ とおく．このとき，(ii) により

$$I(V) \ni v \Longrightarrow C_G(v) \subseteqq N$$

である．また，(ii) により $C_G(V)=V$ であるから，4 元群の自己同型群を考えて，$|N/V|=2$ または 6 であるが，$I(V)\ni v, v_1$，$v\neq v_1$ とすると，$C_G(v), C_G(v_1)\triangleright V$ であるから，N は少なくとも二つの異なる Sylow 2 部分群をもち，$|N/V|=6$ でなければならない．このとき，$N\simeq\mathfrak{S}_4$ (4 次対称群) をみるのは難しくない．さて，G の位数 2 の元の $N\backslash G$ における分布を調べよう．

(8.74) $I(G)-N\ni u$ のとき，

$$C_G(u)\cap N \neq 1 \Longleftrightarrow |N\cap N^u| = 4 \Longleftrightarrow |Nu\cap I(G)| = 2$$

である．実際，$C_G(u)\cap N\neq 1$ ならば，$v\in I(C_G(u)\cap N)$ とするとき，$v\in N-V$ で，$C_N(v)$ は 4 元群である．$C_N(v)\triangleleft C_G(v)$, $u\in C_G(v)$ より $C_N(v)\subseteqq N\cap N^u$ であるが，$N\simeq\mathfrak{S}_4$ の性質から $C_N(v)=N\cap N^u$，よって $|N\cap N^u|=4$ である．u は $N\cap N^u$ のちょうど 2 個の元 (1 と v) を逆転するから，(8.72) により，$|I(G)\cap Nu|=2$ である．逆に $|I(G)\cap Nu|=2$ とすると，(8.72) により N は u によって逆転される元をちょうど 2 個もつから，その一つは位数 2 でなければならない．よって $C_G(u)\cap N\neq 1$ である．これで (8.74) が示された．(8.74) と補題 8.21 から

(8.75) $\qquad I(G)-N\ni u \Longrightarrow |N\cap N^u| = 1,\ 3$ または 4

であることがわかる．さらに (8.72), (8.75) により

(8.76) $|N\cap N^u|=1$, 3 または 4 に従って $|I(G)\cap Nu|=1$, 3 または 2

である．さて，$n=0,1,2,3$ に対して，$|Nx\cap I(G)|=n$, $N\neq Nx$ なる右剰余類 Nx の個数を b_n としよう．明らかに

$$1+b_0+b_1+b_2+b_3=\frac{|G|}{24} \tag{8.77}$$

である．また $|I(G)|=|G|/8$, $|I(N)|=9$ に注意すると，

$$9+b_1+2b_2+3b_3=\frac{|G|}{8} \tag{8.78}$$

である．さらにつぎが成り立つ：

$$b_0=b_1=0,\quad b_2=6. \tag{8.79}$$

実際，(8.74) の証明からわかるように，$I(N)-V$ の元と $|Nx\cap I(G)|=2$ なる Nx は1対1に対応するから，b_2 は $|I(N)-V|=6$ に等しい．このとき，(8.77)，(8.78) から，$3b_0+2b_1=0$．よって $b_0=b_1=0$ である．

したがって，$21+3b_3=|G|/8$ であるから，$b_3=0$ ならば $|G|=168$ である．$b_3\neq 0$ としよう．まず，$3b_3$ は $|N\cap N^u|=3$ なる $I(G)-N$ の元 u の数に等しいことに注意する：

$$3b_3=|\{u\in I(G)-N\,|\,|N\cap N^u|=3\}|. \tag{8.80}$$

そこで，N の位数3の部分群 T をとり，T の各元を逆転する $I(G)-N$ の元の個数を数えよう．u をそのような元の一つとする．$N\simeq\mathfrak{S}_4$ の性質により，N は T の各元を逆転する位数2の元 t を含む．このとき，$tu\in C_G(T)$, $tu\notin N$ であるから，$C_G(T)\subsetneq N$ である．$A=C_G(T)$, $H=N_G(T)$ とおくと，$[H:A]=2$, $t\in H$ である．(i), (ii) により $C_G(t)$ は2群，A は奇数位数であるから，t は A に固定点なしに作用する．よって (8.73) により，A は Abel 群で t は A の各元を逆転する．また，$I(N_G(A))\ni v$ とすると (ii) により v は A に固定点なしに作用し，よって (8.73) により v は A の各元とくに T の各元を逆転するから，$v\in N_G(T)=H$ である．よって $I(N_G(A))=I(H)$ で，$I(H)$ の各元は A の各元を逆転する．したがって $|I(H)|=|A|$ であるから，T の各元を逆転する位数2の元は $|A|$ 個あることがわかる．そのうち3個は N に含まれるから，T の各元を逆転する $I(G)-N$ の元の個数は $|A|-3$ 個である．ところで，T_1, T_2 を N の異なる位数3の部分群とするとき，$|Nx\cap I(G)|\leqq 3$ $(N\neq Nx)$ より T_1 の各元を逆転する $I(G)-N$ の元の集合と，T_2 の各元を逆転する $I(G)-N$ の元の集合は共通

部分がない．よって，N は位数 3 の部分群を 4 個含むことに注意すると，(8.80) により $3b_3=4(|A|-3)$，したがって

$$4|A|+9=\frac{|G|}{8} \tag{8.81}$$

を得る．さて，こんどは $H\backslash G$ における位数 2 の元の分布を調べよう．$|I(H)|=|A|$ で，$I(H)$ の各元 v は $I(G)-H$ のちょうど 4 個の元と交換可能 ($|I(C_G(v))|=5$ に注意) である．しかも $I(H)\ni v_1, v_2\,(v_1\neq v_2)$ ならば，$v_1v_2\in A$ (奇数位数) であるから，$C_G(v_1)\cap C_G(v_2)=1$．したがって，$G-H$ は少なくとも $4|A|$ 個の位数 2 の元を含む．よって，(8.81) により

$$|A|+4|A|\leqq 4|A|+9, \qquad \therefore \quad |A|\leqq 9.$$

一方，$|A|=$奇数，$|A|>|T|=3$ より，$|A|\geqq 9$ であるから，結局 $|A|=9$ でなければならない．このとき (8.81) から，$|G|=360$ を得る．▌

さて，(8.70) からつぎの補題が得られる．これも位数 2 の元の取り扱いの際にしばしば用いられる有用な補題である．

補題 8.22 $I(G)\ni u, v$ とする．

(i) uv の位数が奇数ならば，u と v は $\langle u, v\rangle$ で共役である．

(ii) uv の位数が偶数ならば，$[u, z]=[v, z]=1$ なる位数 2 の元 z が存在する．ここで [,] は交換子を表わす．

証明 $|uv|=n$ とする．(8.70) により $\langle u, v\rangle$ は位数 $2n$ の正 2 面体群 D_{2n} である．n が偶数ならば，$(uv)^{n/2}=z$ は D_{2n} の中心に含まれるから z は (ii) を満たす．n が奇数ならば D_{2n} の共役類を調べて (あるいは Sylow の定理 2.3 から)，位数 2 の元は D_{2n} ですべて共役である．▌

例題 8.6 G を偶数位数の群，$i(G)\geqq 2$ とする．$n=\max\{|C_G(x)|\mid x\in I(G)\}$ とおくと，$|G|<n^3$．

[証明] x を $n=|C_G(x)|$ なる位数 2 の元とする．$m=[G:C_G(x)]$ とおくと，x を含む G の共役類 K は m 個の元を含む．仮定により，x と共役でない位数 2 の元 y が存在する．

$$I(C_G(y))=\{y_1, y_2, \cdots, y_t\}$$

とするとき，

$$(*)\qquad K \subseteqq \bigcup_{i=1}^{t} C_G(y_i)$$

である．実際，$K \ni x'$ とするとき，x' と y は共役でないから，補題 8.22 により $[x', z]=[y, z]=1$ なる $z \in I(G)$ が存在する．このとき $z \in I(C_G(y))$．よって $x' \in \bigcup_{i=1}^{t} C_G(y_i)$ である．さて，(＊)の両辺における元の数を比較すると，$|C_G(y_i)| \leqq n$ $(i=1, 2, \cdots, t)$，$t<|C_G(y)| \leqq n$ に注意して

$$m < tn < n^2$$

を得る．したがって $|G|=mn<n^3$ である．▌

この例題において，$x \notin Z(G)$ $(n=|C_G(x)|)$ ならば，G は $|H|>|G|^{1/3}$ なる真の部分群 H をもつことになる．実は，Brauer-Fowler は (8.70) に基づく counting argument により，位数が 2 より大きい任意の偶数位数の群に対してこの事実が成り立つことを証明した．ここでは，§8.5 で証明した Frobenius-Schur の定理の応用として，これを証明しよう．

注意　素数位数でない可解群 G は，$|G|^{1/2} \leqq |H|$ なる真の部分群 H をもつ．これは定理 7.2 からわかる．したがって，奇数位数の群の可解性を用いれば，素数位数でない任意の有限群は，$|G|^{1/3}<|H|$ なる真の部分群 H をもつことになる．なお，位数が 2 より大きい偶数位数の群に対しても $|G|^{1/2} \leqq |H|$ なる真の部分群 H の存在が予想されているようである．

G の既約指標 χ に対して

$$\nu(\chi) = \frac{1}{|G|}\sum_{x \in G} \chi(x^2)$$

とおく．Frobenius-Schur の定理 8.25 により

$$(8.82)\qquad \nu(\chi) = \begin{cases} 0 & (\chi \neq \bar{\chi}), \\ \pm 1 & (\chi = \bar{\chi}) \end{cases}$$

である．

補題 8.23
$$|I(G)|+1 = \sum_{\chi \in \mathrm{Irr}(G)} \nu(\chi)\chi(1).$$

証明　$G \ni x$ に対して，$y^2=x$ となる y の個数を $\theta(x)$ としよう：

$$\theta(x) = |\{y \in G \mid y^2=x\}|.$$

明らかに，$\theta(x)$ は G の類関数であるから，

$$\theta(x) = \sum_{\chi \in \mathrm{Irr}(G)} c_\chi \chi(x) \qquad (c_\chi \in \boldsymbol{C})$$

と書ける．直交関係により

$$c_\chi=(\theta,\chi)=\frac{1}{|G|}\sum_{x\in G}\theta(x)\overline{\chi(x)}.$$

ところで，$\theta(x)\overline{\chi}(x)=\sum_{\substack{G\ni y\\ y^2=x}}\overline{\chi(y^2)}$ であるから

$$c_\chi=\frac{1}{|G|}\sum_{y\in G}\overline{\chi(y^2)}=\frac{1}{|G|}\sum_{y\in G}\chi(y^{-2})=\frac{1}{|G|}\sum_{y\in G}\chi(y^2)=\nu(\chi)$$

を得る．よって

$$\theta=\sum_{\chi\in\mathrm{Irr}\,(G)}\nu(\chi)\chi$$

であるが，明らかに $\theta(1)=|I(G)|+1$ であるから，

$$|I(G)|+1=\theta(1)=\sum_{\chi\in\mathrm{Irr}\,(G)}\nu(\chi)\chi(1)$$

を得る．▌

問 8.28 正整数 n に対して

$$\nu_n(\chi)=\frac{1}{|G|}\sum_{x\in G}\chi(x^n)\qquad(\chi\in\mathrm{Irr}\,(G)),$$

$$I_n(G)=\{x\in G\mid x^n=1\}$$

とおくとき，

$$|I_n(G)|+1=\sum_{\chi\in\mathrm{Irr}\,(G)}\nu_n(\chi)\chi(1)$$

を示せ．(注意: $\nu_n(\chi)$ は整数であることが知られているが，一般の n に対してはその値は $n=2$ のときのようにはっきりしていない．つぎの問 8.29 参照.)

問 8.29 標数 p の素体に成分をもつつぎの形の行列全体の作る群を G とする：

$$\begin{bmatrix}1 & * & *\\ 0 & E_n & *\\ 0 & 0 & 1\end{bmatrix}\in GL(n+2,p).$$

このとき，つぎを示せ：

(i) G は p^{2n} 個の 1 次指標と $p-1$ 個の p^n 次既約指標をもつ．

(ii) χ を p^n 次既約指標とするとき，p が奇素数ならば $\nu_p(\chi)=p^n$，$p=2$ ならば $\nu_4(\chi)=2^n$ を示せ．($\nu_2(\chi)=0,\ \pm1$ であるのに反して $\nu_p(\chi)$ (p: 奇素数) はいくらでも大きな値がとれることに注意.)

補題 8.24 G を偶数位数の群，$n=(|G|-1)/|I(G)|$ とおく．このとき，$[G:$

$C_G(x)]\leqq n^2$ なる $1\neq x\in G$ が存在する.

証明 $$\mathcal{R}=\{\chi\in \mathrm{Irr}(G)\mid \chi=\bar{\chi}\neq 1_G\}$$

とおくと, 補題8.23と(8.82)により

$$0<\frac{|G|-1}{n}=|I(G)|\leqq \sum_{\chi\in\mathcal{R}}\chi(1)$$

である. よって $|\mathcal{R}|=r$ とすると

$$|I(G)|^2\leqq\left(\sum_{\chi\in\mathcal{R}}\chi(1)\right)^2\leqq r\sum_{\chi\in\mathcal{R}}\chi(1)^2\leqq r(|G|-1)$$

を得る. ここで第2の不等号は有名な Schwarz の不等式から得られ, 第3の不等号は直交関係から得られる. よって

$$|G|-1\leqq rn^2$$

であるが, $r\leqq|\mathrm{Irr}(G)|-1$ より

$$(*)\qquad |G|-1\leqq(|\mathrm{Irr}(G)|-1)n^2$$

を得る. ところで, $|\mathrm{Irr}(G)|-1$ は G の自明でない共役類の数であるから, $(*)$ は $|K|\leqq n^2$ なる共役類 K が存在することを示す. このとき, $K\ni x$ とすれば $[G:C_G(x)]\leqq n^2$ である. ▌

問 8.30 補題8.24の記号を用いる. このとき, $\chi(1)\leqq n$, $1\neq\chi=\bar{\chi}$ なる既約指標の存在を示せ. [ヒント] 補題8.24の証明をよくみよ.

定理 8.36 (Brauer-Fowler) G を偶数位数 (>2) の群とするとき, $|G|^{1/3}<|H|$ なる真の部分群 H が存在する.

証明 G の位数に関する数学的帰納法による. $Z(G)\neq 1$, $G/Z(G)$ が偶数位数ならば, $|G/Z(G)|^{1/3}<|H/Z(G)|$ なる G の真の部分群 H が存在する. このとき, H が求めるものである. $Z(G)\neq 1$, $G/Z(G)$ が奇数位数ならば, $\mathrm{Syl}_2(G)\ni P$ とすると $P\subseteqq Z(G)$. よって Schur-Zassenhaus の定理(定理7.1)を用いて $G=P\otimes L$ となる. とくに G は指数2の部分群 H をもち, $|H|\geqq|G|^{1/2}>|G|^{1/3}$ である. したがって $Z(G)=1$ としてよい. このとき, 補題8.24により

$$1<[G:C_G(x)]\leqq n^2\qquad\left(n=\frac{|G|-1}{|I(G)|}\right)$$

なる $x\in G$ が存在する. $n^2<|G|^{2/3}$ ならば $H=C_G(x)$ が求めるものである. $n^2\geqq|G|^{2/3}$ ならば $y\in I(G)$ とするとき,

$$1 < [G:C_G(y)] \leqq |I(G)| = \frac{|G|-1}{n} < \frac{|G|}{n} \leqq |G|^{2/3}$$

となり，$H=C_G(y)$ が求めるものである．▌

補題 8.24 から，1950 年以降の有限単純群の分類問題の指導原理となっているつぎの結果が得られる．

定理 8.37 (Brauer-Fowler) 任意の (偶数位数の) 有限単純群 G と G の任意の位数 2 の元 x に対して

$$|G| \leqq f(|C_G(x)|)$$

を満たす G によらない関数 f が存在する．

証明 G を偶数位数の単純群，$y \in I(G)$ とする．$|C_G(y)|=h$ とすると，

$$\frac{|G|}{h} \leqq |I(G)| = \frac{|G|-1}{n} \qquad \left(n=\frac{|G|-1}{|I(G)|}\right)$$

より $h>n$ である．補題 8.24 により $[G:C_G(x)]\leqq n^2$ なる $1\neq x \in G$ が存在するから，G の $G/C_G(x)$ の上での置換表現を考えると，(G の単純性に注意して) G は n^2 次交代群の部分群と同型である．したがって

$$|G| \leqq \frac{n^2!}{2} < \frac{h^2!}{2}$$

となり，

$$f(h) = \frac{h^2!}{2}$$

とおけばよい．▌

定理 8.37 における関数は，非常に大きな値をとる関数であり実用的ではないが，少なくともつぎのことを示している：

C を $Z(C)$ が偶数位数である有限群とするとき，

(＊) $$C \simeq C_G(x) \qquad (\exists x \in I(G))$$

なる位数 2 の元 x をもつ有限単純群 G は有限個しか存在しない．

このことから

(＊＊) 上のような C が与えられたとき，(＊) を満たす有限単純群を決定せよというわゆる“位数 2 の元の中心化群による有限単純群の特徴づけ”の問題が生じる．(上の例題 8.4–8.5 はこの問題 (＊＊) に対するもっとも簡単な例である.) 問題 (＊＊) は，1950 年以降 Brauer, Suzuki を始めとして，多くの人の努力によ

り既知の有限単純群の殆どすべてに対して解決されており，またその過程で現在‘散在型単純群(sporadic simple groups)’とよばれているいくつかの単純群が発見された．これらの結果については，

都筑，木村，坂内，近藤：有限群論の現状，雑誌“科学”1974年9月号(岩波書店)

に綜合報告があるので参照されたい．さて，問題(∗∗)では C の構造を具体的に与えているのであるから，当然つぎの(∗∗∗)が自然な問題として生じる：

(∗∗∗)　有限単純群の位数2の元の中心化群はどのような構造をもつであろうか．

この問題(∗∗∗)については，1974年秋の札幌における国際シンポジウムにおいて，M. Aschbacher が，いわゆる成分型の群(その定義は，p. 211 を参照)に対して画期的な結果を発表し，有限単純群の分類問題に大きな進歩をもたらした．このように有限単純群の位数2の元の中心化群に注目することは，有限単純群の分類問題の基本的方向となっているのであるが，定理8.37はそのような方向の指針となる原理を示しているわけである．——

最後に，I を G の位数2の元からなる共役類とするとき，G の元 x を

$$x = uv \qquad (u, v \in I)$$

と書き表わす順列 (u, v) の数 $\beta_I(x)$ を指標によって表わす公式を与えて，この項を終りにしよう．

$K_1, K_2, \cdots, K_h$ を G の共役類の全体，$\hat{K}_1, \hat{K}_2, \cdots, \hat{K}_h$ を

$$\hat{K}_i = \sum_{x \in K_i} x$$

なる整数環上の群環 $\boldsymbol{Z}[G]$ の元とする．このとき，

$$\hat{K}_i \cdot \hat{K}_j = \sum_{k=1}^{h} a_{ijk} \hat{K}_k$$

と書ける．ここで a_{ijk} は，$K_k \ni x$ を固定するとき，$x = yz$ $(y \in K_i,\ z \in K_j)$ と書き表わす順列 (y, z) の数である．さて，G の既約指標 χ に対して

$$\omega_\chi(\hat{K}_i) = \frac{|K_i|\chi(x_i)}{\chi(1)} \qquad (x_i \in K_i)$$

とおくと，§8.3, c)，(8.35)により

$$\omega_\chi(\hat{K}_i)\omega_\chi(\hat{K}_j) = \omega_\chi(\hat{K}_i\hat{K}_j) = \sum_{i=1}^{h} a_{ijk}\omega_\chi(\hat{K}_k)$$

である．したがって

$$\frac{|K_i||K_j|\chi(x_i)\chi(x_j)}{\chi(1)} = \sum_{k=1}^{h} a_{ijk}|K_k|\chi(x_k)$$

であるが，両辺に $\overline{\chi(x_n)}$ を掛けてすべての既約指標 χ について加えると

$$\begin{aligned}\sum_{\chi\in \mathrm{Irr}(G)} \frac{|K_i||K_j|\chi(x_i)\chi(x_j)\overline{\chi(x_n)}}{\chi(1)} &= \sum_{\chi}\sum_{k} a_{ijk}|K_k|\chi(x_k)\overline{\chi(x_n)} \\ &= \sum_{k} a_{ijk}|K_k|\Big(\sum_{\chi}\chi(x_k)\overline{\chi(x_n)}\Big) \\ &= a_{ijn}|G| \qquad (\text{第 2 直交関係}).\end{aligned}$$

よって，

$$a_{ijn} = \frac{|K_i||K_j|}{|G|}\sum_{\chi\in \mathrm{Irr}(G)}\frac{\chi(x_i)\chi(x_j)\overline{\chi(x_n)}}{\chi(1)}$$

を得る．ここで，$K_i=K_j=I$ とすると，

$$\beta_I(x) = \frac{|I|^2}{|G|}\sum_{\chi\in \mathrm{Irr}(G)}\frac{\chi(t)^2\overline{\chi(x)}}{\chi(1)} \qquad (t\in I) \tag{8.83}$$

を得る．$\beta_I(x)$ は x を逆転する I の元の数であるから，それは G の群論的性質からあらかじめわかることがしばしば起こり，そのとき (8.83) は群指標の間の関係式を与えたり，あるいは G の位数についての情報を与えることを示している．

例題 8.7 G をその Sylow 2 部分群が 4 元数型の群である有限群とするとき，偶数位数の元 x に対して $\beta_I(x)=0$.

証明 $\beta_I(x)\neq 0$ すなわち $x=uv$ $(u, v\in I(G))$ とすると，$\langle u, v\rangle=\langle u, x\rangle$ は正 2 面体群である．よって $\langle u, v\rangle$ は 4 元群を含む．とくに Sylow の定理により，G の Sylow 2 部分群は 4 元群を含む．しかるに 4 元数型の群は，位数 2 の元をただ一つしか含まないから，4 元群を含み得ず矛盾である．▌

b）4 元数型の Sylow 2 部分群をもつ有限群

この項では，本節の a) および §8.7 の補題 8.17 の応用として，Brauer-Suzuki によるつぎの定理 8.38 を証明する．近年，与えられた 2 群を Sylow 2 部分群とする有限群を決定するという問題に対して，著しい進歩がなされているが，こ

の定理 8.38 は，そのような結果としては，現代の有限群論の得た最初のものであり，最近の有限単純群論において基本的役割を果たしているものである．

定理 8.38 (Brauer-Suzuki)　G を，4 元数型の 2 群を Sylow 2 部分群とする有限群とするとき，

$$G \triangleright \langle t\rangle O(G) \qquad (\forall t \in I(G))$$

である．ここで，$O(G)$ は G の奇数位数の最大正規部分群を表わす．とくに，4 元数型の 2 群を Sylow 2 部分群とする有限群は単純群ではない．——

実際に証明されるのは，つぎの命題である：

(8.84)　G を，4 元数型の Sylow 2 部分群をもつ群とするとき，G の自明でない既約指標 χ が存在して $\chi(1)=\chi(t)$ $(t \in I(G))$.

最初に，定理 8.38 は (8.84) の系であることを示しておこう．G の位数に関する帰納法を用いる．$O(G)=1$ としてよい．(8.84) におけるように既約指標 χ をとり，$N=\mathrm{Ker}\,\chi$ とおくと $G \gneqq N \ni t$ である．$O(N) \subseteqq O(G)=1$ より $O(N)=1$ である．$N \triangleright \langle t\rangle$ を示そう．4 元数型の群の部分群は巡回群か 4 元数型の群のいずれかであるから，$\mathrm{Syl}_2(N) \ni S$ とするとき，S も巡回群か 4 元数型の群かのいずれかである．S が巡回群ならば，例題 7.5 の (i) および $O(N)=1$ より $N=S$ となり $N \triangleright \langle t\rangle$ である．S が 4 元数型の群ならば，帰納法の仮定により $N \triangleright \langle t\rangle O(N) =\langle t\rangle$ を得る．$N \triangleright \langle t\rangle$ は，t が N のただ一つの位数 2 の元であることを示すから，$G \triangleright \langle t\rangle$ でなければならない．——

$\mathrm{Syl}_2(G) \ni Q$, $|Q|=2^{n+1}$ $(n \geqq 2)$ とすると，Q は

$$a^{2^n}=1, \quad b^2=a^{2^{n-1}}, \quad b^{-1}ab=a^{-1}$$

なる生成元 a, b をもつ．

$$t=a^{2^{n-1}}, \quad P=\langle a^{2^{n-2}}\rangle, \quad H=N_G(P)$$

とおくと，t は位数 2 の元，$|P|=4$ である．以下，(8.84) をいくつかの段階に分けて証明しよう．

(α)　H は 2 巾零である．

[証明]　$C_G(P)$ の Sylow 2 部分群は，巡回群 $\langle a\rangle$ であるから，例題 7.5 の (i) により $C_G(P)$ は 2 巾零である．ところが，$[H : C_G(P)]=2$ であるから，$H=N_G(P)$ も 2 巾零でなければならない．▌

(α) により

$$H = SU \triangleright U, \quad S \cap U = 1$$

なる奇数位数の部分群 U が存在する．このとき，

(8.85) $$[a^{2^{n-2}}, U] = 1$$

であることは容易にわかる．

$$W = \langle a \rangle U, \quad V = \langle t \rangle U, \quad D = W - V$$

とおく．

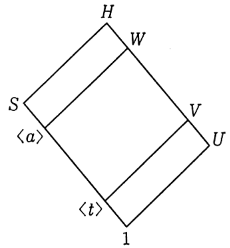


図 6

(β) D は G の TI 集合で，$H = N_G(D)$.

[証明] D の任意の元は適当な巾を作ると $a^{2^{n-2}}$ となる．実際，$D \ni a^i u$ ($u \in U$, $i \neq 0$) とすると，$a^i u$ の適当な巾は $a^{2^{n-2}}u'$ ($u' \in U$) となり，(8.85) により $a^{2^{n-2}}$ と u' は可換で $|u'|$ は奇数であるから，$a^{2^{n-2}}u'$ の適当な奇数巾は $a^{2^{n-2}}$ となる．さて，$D \ni y, z$, $y^x = z$ ($x \in G$) とすると，$y^x = z$ の両辺の適当な巾を作れば，$(a^{2^{n-2}})^x = a^{\pm 2^{n-2}}$ となる．$(a^{2^{n-2}})^x = a^{2^{n-2}}$ ならば $x \in C_G(P) \subseteqq H$, $(a^{2^{n-2}})^x = a^{-2^{n-2}}$ ならば $xb \in C_G(P) \subseteqq H$, よって $x \in H$. すなわち D は補題 8.16 の (ii) を満たす．上の推論で $y = z$ とすると，補題 8.16 の (i) がでるから，D は TI 集合で $H = N_G(D)$ である．▌

(γ) $n \geqq 3$ のとき，(8.84) が成り立つ．

[証明] $n \geqq 3$ のとき，H/V は位数 2^n ($\geqq 8$) の正 2 面体群である．位数 2 の群 H/W の自明でない 1 次指標 φ と H/V の 2 次既約指標 ψ をとる．このとき，$1_H + \varphi - \psi \in M_H(D)$ である．実際，V の上では $\mathrm{Ker}\,\varphi, \mathrm{Ker}\,\psi \subseteqq V$ より $1_H(u) + \varphi(u) - \psi(u) = 1 + 1 - 2 = 0$ であり，$H - W \ni u$ ならば $1_H(u) + \varphi(u) - \psi(u) = 1 - 1 - 0 = 0$ である．$\theta = 1_H + \varphi - \psi$ とおくと，$(\theta, \theta)_H = 3$ であるから，補題 8.17 により，$(\theta^G, \theta^G)_G = 3$ である．また Frobenius 相互律により $(\theta^G, 1_G) = (\theta, 1_H) = 1$

であるから，$\theta^G(1)=0$ に注意して

$$\theta^G = 1_G+\Phi-\Psi \qquad (\Phi, \Psi \in \mathrm{Irr}(G))$$

なる分解が得られる．$D^G \ni y$ ならば $\theta^G(y)=0$ であるから，とくに

$$(8.86) \qquad \begin{cases} 1+\Phi(1)-\Psi(1) = 0, \\ 1+\Phi(t)-\Psi(t) = 0 \end{cases}$$

である．$I=I(G)$ としよう．本節 a) の最後でみたように

$$\beta_I(x) = \frac{|I|^2}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(t)^2\overline{\chi(x)}}{\chi(1)}$$

であるが，$D^G \ni x$ ならば x は偶数位数であるから，例題8.7により $\beta_I(x)=0$，したがって

$$(\beta_I, \theta^G) = \frac{1}{|G|}\sum_{x\in G}\beta_I(x)\overline{\theta^G(x)}$$

の各項(のどちらかの因子)が0となり，$(\beta_I, \theta^G)=0$ を得る．したがって

$$0 = (\beta_I, \theta^G) = (\beta_I, 1_G+\Phi-\Psi) = \frac{|I|^2}{|G|^2}\left(1+\frac{\Phi(t)^2}{\Phi(1)}-\frac{\Psi(t)^2}{\Psi(1)}\right)$$

より，

$$1+\frac{\Phi(t)^2}{\Phi(1)}-\frac{\Psi(t)^2}{\Psi(1)} = 0$$

を得る．$\Phi(1)=f$，$\Phi(t)=x$ とおくと，(8.86) より $\Psi(1)=1+f$，$\Psi(t)=1+x$ であるから，

$$1+\frac{x^2}{f}-\frac{(x+1)^2}{f+1} = 0$$

を得る．これから $f=x$ すなわち $\Phi(1)=\Phi(t)$ が得られ，$n\geqq 3$ の場合に (8.84) が証明された．▌

以下，$n=2$ とする．このとき

$$Q = \langle a, b \mid a^2=b^2,\ a^4=1,\ b^{-1}ab=a^{-1}\rangle,$$
$$P = \langle a\rangle, \qquad t = a^2$$

である．$n=2$ であるから H/V は4元群となる．H/V の4つの1次指標を 1_H，$\varphi_1, \varphi_2, \varphi_3$ とし，φ_1 は W を核に含むものとする．このとき，

$$\theta = 1_H+\varphi_1-\varphi_2-\varphi_3 \in M_H(D)$$

であることは見易い．補題8.17により，$(\theta^G, \theta^G)=(\theta, \theta)=4$，Frobenius 相互律

により，$(\theta^G, 1_G)=(\theta, 1_H)=1$ であるから，

$$\theta^G = 1+\varepsilon_1\chi_1+\varepsilon_2\chi_2+\varepsilon_3\chi_3 \qquad (\chi_i \in \mathrm{Irr}(G),\ \varepsilon_i=\pm 1) \tag{8.87}$$

なる分解が得られる．

(δ) (i) $\theta^G(x) = \begin{cases} 0 & (x \notin D^G), \\ 4 & (x \in D^G). \end{cases}$

(ii) $1+\sum_{i=1}^{3}\dfrac{\varepsilon_i\chi_i(t)^2}{\chi_i(1)} = 0.$

[証明] $\theta^G(x)=0$ $(x \notin D^G)$ は明らかであり，$\theta^G(x)=4$ $(x \in D^G)$ は，補題 8.17 からでる．(ii) は，(γ) におけるように $(\beta_I, \theta^G)=0$ からでる．▌

$$\chi_i(1) = x_i, \qquad \chi_i(t) = y_i, \qquad z_i = x_i - y_i \qquad (i=1, 2, 3)$$

とおく．(δ) の (i), (ii) を書きかえて

$$1+\varepsilon_1x_1+\varepsilon_2x_2+\varepsilon_3x_3 = 0 \qquad (\theta^G(1)=0 \text{ による}), \tag{8.88}$$

$$\sum_{i=1}^{3}\varepsilon_iz_i = 0 \qquad (\theta^G(1)-\theta^G(t)=0 \text{ による}), \tag{8.89}$$

$$\sum_{i=1}^{3}\frac{\varepsilon_iz_i^2}{x_i} = 0 \qquad ((\delta) \text{ の (ii) および (8.88), (8.89)}) \tag{8.90}$$

を得る．或る i に対して $z_i=0$ あるいは或る j に対して $x_j=1$ が示されれば (8.84) が成り立つから，以後

$$z_i \neq 0, \qquad x_i > 1 \qquad (i=1, 2, 3)$$

と仮定して矛盾を導こう．

注意 ここで述べる $n=2$ の場合の証明は G. Glauberman によるものである．Brauer-Suzuki の定理 8.38 の原証明では，$n=2$ の場合にはモジュラー表現の理論が用いられていた．$n\geqq 3$ のときに比べて，$n=2$ のときは補題 8.17 に基づいて得られる関係式の数が十分ではないために，(8.84) の証明が面倒になるのである．事実以下の証明は，$n\geqq 3$ のときの明快さに比べ極めて技巧的である．

(ε) (i) χ_i $(1\leqq i\leqq 3)$ は G の各元に対して整数値をとる．

(ii) $\chi_i(au) = \chi_i(au^{-1})$ $(\forall u \in U)$.

[証明] χ_1 が G の或る元に対して整数値でないとする．有理数体 $\boldsymbol{Q}$ に 1 の原始 $|G|$ 乗根を添加した体 K の自己同型 σ を適当にとると $\chi_1^\sigma \neq \chi_1$ である．ここで χ_1^σ は $\chi_1^\sigma(x)=\chi_1(x)^\sigma$ $(x \in G)$ によって定義される G の既約指標である．このとき，

$$\begin{aligned}(\theta^G, \chi_1{}^\sigma) &= ((\theta^G)^\sigma, \chi_1{}^\sigma) \qquad (\theta^G \text{ は整数値をとる}) \\ &= (\theta^G, \chi_1) \\ &= \varepsilon_1\end{aligned}$$

であるから，θ^G の分解(8.87)と比べて，$j=2$ または3に対して $\chi_1{}^\sigma=\chi_j$，$\varepsilon_1=\varepsilon_j$ である．$j=2$ として一般性を失わない．このとき，$x_1=x_2$，$y_1=y_2$，よって $z_1=z_2$ である．(8.89), (8.90)により

$$0 = 2\varepsilon_1 z_1 + \varepsilon_3 z_3 = \frac{2\varepsilon_1 z_1{}^2}{x_1} + \frac{\varepsilon_3 z_3{}^2}{x_3}$$

であるから，

$$\left(\frac{2\varepsilon_1}{x_1} + \frac{4\varepsilon_3}{x_3}\right) z_1{}^2 = 0$$

を得るが，$z_1 \neq 0$ と仮定しているから $\varepsilon_3 x_3 = -2\varepsilon_1 x_1$．このとき，

$$1+\varepsilon_1 x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3 = 1 + 2\varepsilon_1 x_1 - 2\varepsilon_1 x_1 = 1$$

となり(8.88)に反する．したがって(i)が証明された．K の自己同型 σ で原始4乗根を自分自身に移し，1の奇数巾根を逆数に移すものが存在する．このとき，χ_i を指標とする K 上の行列表現を考えれば，$au=ua$ に注意して((8.85))，$\chi_i{}^\sigma(au)=\chi_i(au^{-1})$ となる．(i)により $\chi_i{}^\sigma=\chi_i$ であるから(ii)が得られる．▌

(ζ) $\chi_i(a)$, $(\chi_i{}^2, \theta^G)$ は奇数である．

[証明] まず G の類関数 φ に対して

(8.91) $$(\varphi, \theta^G) = \frac{1}{|U|}\sum_{u \in U} \varphi(au)$$

であることに注意する．実際，

$$\begin{aligned}(\varphi, \theta^G) &= (\varphi \mid H, \theta) && (\text{Frobenius 相互律}) \\ &= \frac{1}{|H|}\sum_{y \in H} \varphi(y)\overline{\theta(y)} \\ &= \frac{4}{|H|}\sum_{y \in D} \varphi(y) && ((\delta) \text{ の (i) および } \theta \in M_H(D)) \\ &= \frac{4}{|H|}\sum_{u \in U} (\varphi(au) + \varphi(a^{-1}u)) && (D \text{ の定義}) \\ &= \frac{1}{|U|}\sum_{u \in U} \varphi(au)\end{aligned}$$

である．さて，(8.91)により

$$\varepsilon_i = (\chi_i, \theta^G) = \frac{1}{|U|}\sum_{u \in U}\chi_i(au)$$

であるから，

$$|U|\varepsilon_i = \chi_i(a) + \sum(\chi_i(au) + \chi_i(au^{-1})) \qquad (\textstyle\sum \text{ は } u, u^{-1} \text{ の一方のみを走る})$$
$$\equiv \chi_i(a) \pmod 2 \qquad ((\varepsilon) \text{ の (ii) による}).$$

この左辺は奇数であるから，$\chi_i(a)$ は奇数である．また

$$|U|(\chi_i^2, \theta^G) = \sum_{u \in U}\chi_i(au)^2$$
$$\equiv \sum_{u \in U}\chi_i(au) \pmod 2$$
$$= \varepsilon_i|U|$$

より，(χ_i^2, θ^G) は奇数である．▌

(η) $\chi_i(a) = \varepsilon_i \quad (i=1, 2, 3)$.

[証明] $\chi_i(a) \neq \varepsilon_i$ と仮定して矛盾を導こう．$\chi_i(a)$ は奇数であるから $\chi_i(a)^2 > \varepsilon_i\chi_i(a)$ である．このとき

$$(\chi_i^2, \theta^G) = \frac{1}{|U|}\sum_{u \in U}\chi_i(au)^2 \qquad ((8.91) \text{ による})$$
$$> \frac{1}{|U|}\sum_{u \in U}\chi_i(au)$$
$$= \varepsilon_i(\chi_i, \theta^G) \qquad ((8.91) \text{ による})$$
$$= 1.$$

よって，(χ_i^2, θ^G) が奇数であることに注意すると，

(8.92) $$(\chi_i^2, \theta^G) \geqq 3$$

である．また

$$\sum_{y \in G-D^G}\chi_i(y)^2 > -\sum_{y \in G-D^G}\varepsilon_i\chi_i(y) \qquad (\chi_i(1) = x_i > 1 \text{ に注意})$$
$$= \sum_{y \in D^G}\varepsilon_i\chi_i(y) \qquad ((\chi_i, 1^G) = 0 \text{ による})$$
$$= \frac{1}{4}\sum_{y \in G}\varepsilon_i\chi_i(y)\overline{\theta^G(y)} \qquad ((\delta) \text{ の (i) による})$$
$$= \frac{|G|}{4}(\varepsilon_i\chi_i, \theta^G) = \frac{|G|}{4}$$

であるから，

$$|G| = \sum_{y\in G-D^G}\chi_i(y)^2+\sum_{y\in D^G}\chi_i(y)^2 > \frac{|G|}{4}+\frac{1}{4}\sum_{y\in G}\chi_i(y)^2\overline{\theta^G(y)}$$
$$= \frac{|G|}{4}+\frac{|G|}{4}(\chi_i^2, \theta^G)$$
$$\geqq |G| \qquad ((8.92)\text{による})$$

となり矛盾である. ▌

(θ) (i) $z_i \equiv 0 \pmod 4$.

(ii) $x_i \equiv 1 \pmod 2$.

(iii) $z_i \equiv 0 \pmod 8 \Longrightarrow x_i \equiv \varepsilon_i \pmod 4$.

[証明] ψ を Q ($\in \mathrm{Syl}_2(G)$) の2次既約指標とすると,

$$\psi(1) = 2, \quad \psi(t) = -2, \quad \psi(y) = 0 \quad (y \neq 1, t)$$

である. このとき,

$$8(\chi_i\,|\,Q, \psi) = 2x_i-2y_i = 2z_i.$$

これから (i) がでる. (ii), (iii) を示すために, G の位数4の元はすべて共役であることを示そう. Q の位数2または4の部分群(これらは巡回群である)を R とするとき, $N_G(R)/C_G(R)$ は2群である. よって $N_G(Q)/C_G(Q)$ が2群ならば, Frobenius の定理 7.13 により, G は2巾零となり定理 8.38 が成り立つことになる. したがって $N_G(Q)/C_G(Q)$ は2群ではない. このとき, 4元数群 Q の自己同型群を考えると, $3\,|\,|N_G(Q)|/|C_G(Q)|$ となり, Q の位数4の元は $N_G(Q)$ ですべて共役であることがわかる. このことと (η) を用いると

$$8(\chi_i\,|\,Q, 1_Q) = x_i+y_i+6\varepsilon_i$$
$$\equiv 2x_i-z_i-2\varepsilon_i \pmod 8$$
$$\equiv 2(x_i-\varepsilon_i)-z_i \pmod 8.$$

これから x_i は奇数であること, および $z_i\equiv 0 \pmod 8$ ならば, $x_i\equiv\varepsilon_i \pmod 4$ であることがでる. ▌

(θ) を用いて (8.84) の証明を完成させることができる. $z_i\neq 0$ と仮定しているから, z_1, z_2, z_3 のすべてを割る最大2巾を 2^k として,

$$z_i = 2^k w_i$$

とおくと, (θ) の (i) により $k\geqq 2$ であり, w_1, w_2, w_3 の一つは奇数となるから, w_3 が奇数であると仮定する. (8.90) により,

$$\varepsilon_1 x_2 x_3 w_1{}^2 + \varepsilon_2 x_1 x_3 w_2{}^2 + \varepsilon_3 x_1 x_2 w_3{}^2 = 0$$

であり，(θ) の (ii) により x_1, x_2, x_3 が奇数であることに注意すれば，w_1, w_2 の一方は偶数，他方は奇数である．よって，w_1＝偶数，w_2＝奇数とすると，$z_1 \equiv 0 \pmod 8$ である．このとき，

$$\begin{aligned} -\varepsilon_1 x_2 x_3 w_1{}^2 &= \varepsilon_2 x_1 x_3 w_2{}^2 + \varepsilon_3 x_1 x_2 w_3{}^2 \\ &\equiv \varepsilon_2 x_1 x_3 + \varepsilon_3 x_1 x_2 \pmod 4 \\ &\equiv \varepsilon_2 \varepsilon_3 x_1 (\varepsilon_3 x_3 + \varepsilon_2 x_2) \pmod 4 \end{aligned}$$

である．w_1 は偶数であるから，$\varepsilon_3 x_3 + \varepsilon_2 x_2 \equiv 0 \pmod 4$ となり，(8.88) から $1 + \varepsilon_1 x_1 \equiv 0 \pmod 4$ を得る．ところが，$z_1 \equiv 0 \pmod 8$ であるから，これは (θ) の (iii) に矛盾する．これで (8.84)，したがって定理 8.38 の証明が完成した．▌

G の Sylow 2 部分群が 4 元数型の群であるとき，G の構造は決定されている．$O(G)=1$ とするとき，定理 8.38 により $G \triangleright \langle t \rangle$ $(t \in I(G))$ であるが，剰余群 $G/\langle t \rangle$ の Sylow 2 部分群は正 2 面体群となる．ところで，Sylow 2 部分群が正 2 面体群であるような有限群は，Gorenstein-Walter により決定されていて，その結果はつぎの通りである：

Gorenstein-Walter の定理 G を Sylow 2 部分群が正 2 面体群であるような群とするとき，$G/O(G)$ はつぎの群の一つに同型である：

(i) 位数 2 巾の正 2 面体群，

(ii) $PGL(2, q)$ (q: 奇数)，

(iii) $PSL(2, q)$ (q: 奇数)，

(iv) 7 次交代群 $\mathfrak{A}_7$. ——

この定理を用いると，4 元数型の Sylow 2 部分群をもつ有限群を決定するのは，Gorenstein-Walter の定理に現われる群の位数 2 の中心拡大を調べることに帰着し，(i)-(iv) のそれぞれの群に対して一つずつ 4 元数型の Sylow 2 部分群をもつ群が存在する．たとえば，(iii) の群に対しては $SL(2, q)$ が現われるが，詳しいことは省略する．ところで，上の Gorenstein-Walter の定理は，その全証明を本書で取り上げることは不可能であるが，その証明の一部は §8.7-§8.8 で説明してきたことの典型的な応用でもあるので，つぎの項で述べるであろう．

最後に，定理 8.38 に関連していわゆる Glauberman の Z^* 定理に言及してこの項を終りにしよう．1966 年に Glauberman はつぎのような定理を証明した：

Glauberman の Z^* 定理　G を偶数位数の群とする．G の位数2の元 t がつぎの性質(∗)をもつとき，$G \triangleright \langle t\rangle O(G)$ である：

(∗)　$$C_G(t) \ni t^x \quad (x \in G) \Longrightarrow t = t^x.$$ ——

4元数型の Sylow 2部分群をもつ有限群は，その任意の位数2の元が，(∗)を満たすことは明らかであろう．したがって Glauberman の Z^* 定理は定理8.38の一般化である．この Z^* 定理も，有限群論の基本定理の一つなのであるが，その証明は(おそらく本質的に)モジュラー表現の理論が用いられるので，本講では割愛せざるを得ない．しかしそれはモジュラー表現論の応用としては標準的なものでもあるので，興味のある読者は，

G. Glauberman: Central elements in core-free groups, Journal of Algebra **4** (1966), 403-420

を参照されたい．なお，定理8.38は，結果は Z^* 定理の特別の場合であるが，証明は独立にする必要があることに注意しておく．

c) Brauer-Suzuki-Wall の定理

$PSL(2,q)$ (q: 奇数)が，つぎの性質をもつことをみるのは難しくない：

(α)　$PSL(2,q)$ の位数2の元はすべて共役である．

(β)　t を $PSL(2,q)$ の位数2の元とするとき，その中心化群 $C=C_{PSL(2,q)}(t)$ は正2面体群であり，t を含む指数2の巡回部分群を K とするとき，

$$K \cap K^x = 1 \qquad (\forall x \in G-C).$$

(α), (β) から，$PSL(2,q)$ の Sylow 2部分群は正2面体群である．この項では，このことの逆であるつぎの定理を証明する．

定理 8.39 (Brauer-Suzuki-Wall)　G をつぎの性質をもつ偶数位数の群とする：

(i)　G の位数2の元はすべて共役，

(ii)　$I(G) \ni t$，$C=C_G(t)$ とするとき，C はつぎの性質をもつ指数2の部分群 K をもつ：

(ii)′　$C = \langle s\rangle K \ (s \in I(C))$,　$k^s = k^{-1} \ (\forall k \in K)$,　$C_K(s) = \langle t\rangle$,

(ii)″　$K \cap K^x = 1 \quad (\forall x \in G-C)$.

このとき，G はつぎの性質をもつ可換部分群 Q をもつ：

(1)　$|G| = \dfrac{q(q+1)(q-1)}{2}$,　$|Q| = q$,

(2) $Q \ni x \neq 1 \Longrightarrow C_G(x) = Q$,

(3) $[N_G(Q):Q] = (q-1)/2$. また, $N_G(Q)=QD$, $Q \cap D=1$ とおくとき, $N_G(D)$ は位数 $q-1$ の正2面体群で, $D \cap D^x=1$ $(\forall x \in G-N_G(D))$. ——

(i), (ii) から G の Sylow 2 部分群は正2面体群である. しかし (ii)′ により K は Abel 群であるが, 巡回群と仮定してはいない. さて, 証明を始める前に, この定理の意味を説明しておこう.

まず, G を Q の共役全体の集合 Ω の上に作用させるとき, 定理の結論 (1)-(3) から (G, Ω) は §7.2, e) で述べた Zassenhaus 群であることがわかる.

問 8.31 このことを確かめよ. ——

このとき, 置換群論的考察により $G \simeq PSL(2, q)$ が証明される. これについては, 伊藤昇: 有限群論 (共立出版), pp. 127-131 を参照されたい. つぎに定理 8.39 と §8.8, b) で言及した Gorenstein-Walter の定理の証明との関連は, つぎの通りである. G を Sylow 2 部分群が正2面体群である有限群とするとき, Gorenstein-Walter の定理を証明するには, G が単純群であるとき $G \simeq PSL(2, q)$ または $\mathfrak{A}_7$ であることを示せばよいことが, 移送定理や $PSL(2, q)$, $\mathfrak{A}_7$ の自己同型群の性質を用いて比較的容易にわかる. よって G を単純群と仮定する. $I(G) \ni t$ とすると, これまた移送定理の簡単な応用により, $C_G(t)$ は2巾零であることがわかるから,

$$[C_G(t):K] = 2, \qquad K \ni t, \qquad K/O(K) = \text{位数 2 巾の巡回群}$$

なる $C_G(t)$ の部分群 K がただ一つ存在する. このとき, Gorenstein-Walter の定理の証明は, つぎの4段階に分れる:

I $C_G(t), K$ が Brauer-Suzuki-Wall の定理 8.39 の仮定を満たすかあるいは $C_G(t) \simeq C_{\mathfrak{A}_7}((1\ 2)(3\ 4))$ であることを証明する.

II 前者の場合に, G に対して定理 8.39 の結論が成り立つことを示す. すなわち, これが Brauer-Suzuki-Wall の定理である.

III ついで最初に注意したように, 置換群論的考察から $G \simeq PSL(2, q)$ を示す.

IV $C_G(t) \simeq C_{\mathfrak{A}_7}((1\ 2)(3\ 4))$ から $G \simeq \mathfrak{A}_7$ を証明する.

I の証明は, 非常に難解で本講で取り上げることは不可能である. ただしその特別の場合は, D. Gorenstein: Finite Groups, Harper & Row の第15章で解説されているので参照されたい. なお, Gorenstein-Walter が実質的に証明した

のはIであり，II-IVは既にそれ以前に証明されていた．IVは群指標の応用として鈴木通夫氏により証明されている：

M. Suzuki: On finite groups containing an element of order 4 which commutes only with its own powers, Illinois J. Math. **3** (1959), 255-271.

この鈴木氏によるIVの証明も明快なものであるが，本書では割愛する．なお，ここで取り上げる定理8.39の証明は，

H. Bender: Brauer-Suzuki-Wall's Theorem, Illinois J. Math. **18** (1974), 223-228

による．原証明は，ここで与えるものよりは，もっと群指標に依存したもので少し長いが，非常に自然なものなので，興味のある読者は一読することをおすすめする：

R. Brauer, M. Suzuki, G. E. Wall: A characterization of the one-dimensional unimodular projective groups over finite fields, Illinois J. Math. **2** (1958), 718-745.

定理8.39の証明を始めよう．それはいくつかの段階に分けられる．以後，$|K|=k$ とおく．

$$(\alpha)\quad |G| = \frac{q(q-1)(q+1)}{2}, \quad q = 2k+\varepsilon, \quad \varepsilon = \pm 1.$$

[証明]　まず，$k=2$ または 4 のときは，例題8.4，8.5により，$k=2$，$\varepsilon=1$，$|G|=60$，$k=4$，$\varepsilon=-1$，$|G|=168$ あるいは $k=4$，$\varepsilon=1$，$|G|=360$ として (α) が成り立つことに注意する．したがって $k\geqq 6$ と仮定する．以下の証明は，補題8.17の応用であり，定理8.38の(前半の)証明で用いられたのとまったく同じ方法である．

K はAbel群だから，k 個の1次指標をもつ．そのうち $\theta^s=\theta$ なるものがちょうど二つ存在するから(補題8.18)，$k\geqq 6$ に注意すると K は

$$\varphi(t) = 1, \quad \psi(t) = -1, \quad \varphi^s \neq \varphi, \quad \psi^s \neq \psi$$

なる1次指標 φ, ψ をもつことがわかる．このとき，φ^C, ψ^C $(C=C_G(t))$ は C の2次既約指標で

$$\alpha = (1_K - \varphi)^C, \quad \beta = (\varphi - \psi)^C$$

とおくと，

$$\alpha, \beta \in M_G(K^\sharp) \qquad (K^\sharp = K - \{1\})$$

である．そこで補題8.17を用いると

$$\text{(8.93)} \qquad \alpha^G(x) = \alpha(x), \quad \beta^G(x) = \beta(x) \qquad (\forall x \in K),$$

$$\text{とくに} \quad \alpha^G(t) = \alpha(t) = 0, \quad \beta^G(t) = \beta(t) = 4,$$

$$\text{(8.94)} \qquad (\alpha^G, \alpha^G) = (\alpha, \alpha) = 3, \quad (\beta^G, \beta^G) = (\beta, \beta) = 2,$$

$$(\alpha^G, \beta^G) = (\alpha, \beta) = -1$$

である．(8.94)により，α^G, β^G は

$$\text{(8.95)} \quad \alpha^G = 1_G - \varepsilon\Phi + \varepsilon\Lambda, \quad \beta^G = \varepsilon\Phi - \varepsilon\Psi \qquad (\Lambda, \Phi, \Psi \in \mathrm{Irr}(G),\ \varepsilon = \pm 1)$$

なる分解をすることがわかる．$I = I(G)$ とすると，$|I| = [G:C]$ である．(8.83)における類関数 β_I と α^G, β^G の内積を作ると，(8.95)により

$$\text{(8.96)} \quad \begin{aligned} (\alpha^G, \beta_I) &= \frac{|G|}{|C|^2}\left(1 - \frac{\varepsilon\Phi(t)^2}{\Phi(1)} + \frac{\varepsilon\Lambda(t)^2}{\Lambda(1)}\right), \\ (\beta^G, \beta_I) &= \frac{|G|}{|C|^2}\left(\frac{\varepsilon\Phi(t)^2}{\Phi(1)} - \frac{\varepsilon\Psi(t)^2}{\Psi(1)}\right) \end{aligned}$$

を得る．ここで (α^G, β_I), (β^G, β_I) を別の方法で計算しよう．

$$\begin{aligned} (\alpha^G, \beta_I) &= \frac{1}{|G|}\sum_{x \in G} \alpha^G(x)\beta_I(x) \\ &= \frac{1}{|G|}\sum_{x \in \Lambda^G} \alpha^G(x)\beta_I(x) \\ &= \frac{[G:C]}{|G|}\sum_{x \in K} \alpha^G(x)\beta_I(x) \qquad (K \text{ は TI 集合で，} C = N_G(K)) \end{aligned}$$

ところで $x \in K^\sharp$ ならば，$\beta_I(x) = (x$ を逆転する位数2の元の数$) = |Ks| = k$ であるから，

$$\begin{aligned} &= \frac{k}{|C|}\sum_{x \in K} \alpha^G(x) \\ &= \frac{k}{|C|}\sum_{x \in K} \alpha(x) \qquad \text{((8.93) による)} \\ &= \frac{k^2}{|C|}(1_K, \alpha \mid K) \\ &= \frac{2k^2}{|C|} \qquad (\alpha \mid K = (1_K - \varphi) + (1_K - \varphi)^s \text{ に注意}). \end{aligned}$$

同様の計算によって

$$(\beta^G, \beta_I) = 0$$

を得る．よって(8.96)と比べて

$$2k^2 = \frac{|G|}{|C|}\left(1 - \frac{\varepsilon\Phi(t)^2}{\Phi(1)} + \frac{\varepsilon\Lambda(t)^2}{\Lambda(1)}\right), \tag{8.97}$$

$$\Phi(t)^2 - \Psi(t)^2 = 0 \qquad (\Phi(1) = \Psi(1) \text{に注意}) \tag{8.98}$$

である．ところで $\varepsilon\Phi(t) - \varepsilon\Psi(t) = \beta^G(t) = \beta(t) = 4$ であるから，(8.98)より $\Phi(t) = 2\varepsilon$, $\Psi(t) = -2\varepsilon$ を得る．このとき $1 - \varepsilon\Phi(t) + \varepsilon\Lambda(t) = \alpha^G(t) = 0$ より $\Lambda(t) = \varepsilon$ を得る．よって(8.97)から，

$$2k^2\Phi(1)\Lambda(1) = [G:C]f, \qquad f = \Phi(1)\Lambda(1) - 4\varepsilon\Lambda(1) + \varepsilon\Phi(1) \tag{8.99}$$

を得る．ところで，$|C|$ と $[G:C]$ は互いに素であるから(定理の仮定(ii)と補題7.14の証明参照)，(8.99)から

$$[G:C] \mid \Phi(1)\Lambda(1).$$

また，$1 - \varepsilon\Phi(1) + \varepsilon\Lambda(1) = \alpha^G(1) = 0$ より，$\Lambda(1)$ と f は互いに素である．よって，(8.99)から $\Lambda(1) \mid [G:C]$，すなわち $\Lambda(1)$ は奇数で $\Phi(1)$ は偶数であるが，(8.99)より f は8で割れるから $\Phi(1)$ は4で割れない．これから，

$$[G:C] = \frac{\Lambda(1)\Phi(1)}{2}$$

を得るから，(8.99)により

$$4k^2 = f = \varepsilon\Phi(1)(\varepsilon\Lambda(1) + 1) - 4\varepsilon\Lambda(1) = (\varepsilon\Lambda(1) - 1)^2,$$

$$\therefore \quad 2k = \Lambda(1) - \varepsilon.$$

このとき，$\varepsilon\Phi(1) = \varepsilon\Lambda(1) + 1 = \varepsilon(2k + \varepsilon) + 1 = 2k\varepsilon + 2$．よって $\Phi(1) = 2(k + \varepsilon)$ となり

$$[G:C] = (2k + \varepsilon)(k + \varepsilon),$$

$$\therefore \quad |G| = \frac{q(q-1)(q+1)}{2}, \qquad q = 2k + \varepsilon.$$

これで (α) が証明された．▌

以下では群指標は全然用いられず，例題8.4-8.5におけるのと同じ推論によって定理8.39が証明される．まず

$$K^G = C^G \supseteq C_G(y) \qquad (\forall y \in C^G) \tag{8.100}$$

であることに注意する.

(β) $K^G \not\ni x$, $x^t=x^{-1}$ とする. $F=C_G(x)$, $M=N_G(F)$ とおくとき,

(i) $F \ni y \neq 1 \Longrightarrow F=C_G(y)$, $y^t=y^{-1}$,

(ii) $M=F(K\cap M)$, $K\cap M=C_M(t)$,

(iii) $F\cap M^y=1 \quad (\forall y \in G-M)$

(iv) $F\ni y \Longrightarrow \beta_I(y)=|C_G(y)|$.

[証明] (8.100) により $C_G(x)\cap K^G=1$ であるから, t は $F=C_G(x)$ の上に固定点なしに作用する. したがって補題7.18により, F は Abel 群で t は F の各元を逆転する. $F\ni y\neq 1$ とすると $y\notin K^G$, よって $C_G(y)$ は Abel 群となり, とくに $C_G(y)=F$ である. これで(i)が示された. 補題7.14により $|F|$ と $[M:F]$ は互いに素であるから, Schur-Zassenhaus の定理により $t\in D$ なる M/F の補群が存在する. t^y $(y\in D)$ も F の上に固定点なしに作用するから, $t^{-1}t^y\in F$ となり, これは $t=t^y$ を示す. とくに $D=C_M(t)=K\cap M$ すなわち(ii)が示された. (i)により F はTI集合であるから, y を逆転する位数2の元は M に含まれ, tF がそのような元の全体である. よって $\beta_I(y)=|tF|=|C_G(y)|$, すなわち(iv)が成り立つ. (iii)は F がTI集合であることと, $|F|$ と $[M:F]$ が互いに素であることからでる. ▌

(γ) つぎの条件を満たす $G-K^G$ の元 x が存在する:

(i) $x^t=x^{-1}$,

(ii) $\beta_I(x) \geqq \begin{cases} k-1 & (\varepsilon=-1 \text{ のとき}), \\ k+3 & (\varepsilon=1 \text{ のとき}). \end{cases}$

[証明] $I\times I$ から G への写像

$$I\times I\ni (u,v)\longmapsto uv\in G$$

を考えよう. $\beta_I(x)$ は, x に対応する $I\times I$ の元の数であることに注意する. $C^G=K^G\ni x\neq 1$ とすると, x に対応する $I\times I$ の元の個数は k である. また単位元に対応する $I\times I$ の元の数は $[G:C]$ である. K はTI集合で $N_G(K)=C$ であるから, $|K^G-\{1\}|=k[G:C]-[G:C]$ となり, したがって K^G の元に対応する $I\times I$ の元の数は $[G:C]+[G:C](k-1)k$ であるから, K^G の元に対応しない $I\times I$ の元の数は

$$[G:C]^2-([G:C](k-1)k+[G:C])$$

である．$G-K^G$ の元の数は，$|G|-1-[G:C](k-1)$ であるから，

$$\beta_I(x) \geqq \frac{[G:C]^2-([G:C](k-1)k+[G:C])}{|G|-[G:C](k-1)-1}$$

なる $K^G \ni x$ が存在する．右辺を変形しよう．

$$\begin{aligned}(\text{右辺}) &> \frac{[G:C]^2-([G:C](k-1)k+[G:C])}{|G|-[G:C](k-1)} \\ &= \frac{[G:C]-(k-1)k-1}{|C|-(k-1)} \\ &= \frac{(2k+\varepsilon)(k+\varepsilon)-(k-1)k-1}{2k-(k-1)} \\ &= k+\frac{3\varepsilon k}{k+1}.\end{aligned}$$

定理の仮定(i)により $x^t=x^{-1}$ としてよい．このとき，(β) の(iv)により $\beta_I(x)=|C_G(x)|$ であるから

$$|C_G(x)| \geqq k+\frac{3\varepsilon k}{k+1}$$

である．よって $\varepsilon=-1$ ならば $|C_G(x)|\geqq k-2$ であるが，$|C_G(x)|$ は奇数であるから，$|C_G(x)|\geqq k-1$ である．$\varepsilon=1$ ならば $|C_G(x)|\geqq k+3$ である．▌

x を (γ) を満たすようにとり，

$$F=C_G(x), \quad M=N_G(F), \quad |F|=f, \quad [M:F]=n$$

とおく．また G における M の右剰余類 My $(y\in G)$ で M のある位数2の元と可換な元を含むもの全体を $\mathscr{F}$ とする：

$$\mathscr{F}=\{My\in M\backslash G \mid My\cap C_G(u)\neq\phi\ (\exists u\in I(M))\}.$$

このとき，つぎが成り立つ：

(δ)　(i)　$|\mathscr{F}|=\left(\dfrac{2k}{n}-1\right)f+1$,

(ii)　$\displaystyle\sum_{My\in\mathscr{F}}|My\cap I(G)|=f(k+1)$,

(iii)　$|M\backslash G|\equiv|\mathscr{F}| \pmod f$,

(iv)　$M\backslash G-\mathscr{F}\ni My \Longrightarrow |My\cap I(G)|\leqq 1$.

[証明]　(β) の(i)により $|I(M)|=f$ である．また $I(M)\ni u$ ならば (β) の(ii)により $|C_M(u)|=n$ である．$M\neq My$，$My\cap C_G(u)\neq\phi$ $(u\in I(M))$ としよう．$y\in$

$C_M(u)$ としてよい．このとき，$My\cap C_G(u)=C_M(u)y$ である．これは $I(M)$ の各元 u に対して $M\neq My$，$My\cap C_G(u)\neq\phi$ なる My の個数が，$|C_M(u)\backslash C_G(u)|-1=2k/n-1$ であることを示す．一方，$K\simeq C_G(u)\triangleright C_M(u)$ であるから，$C_M(u)\subseteqq M\cap M^y$．このとき (β) の (iii) を用いて $C_M(u)=M\cap M^y=M\cap M^z$ $(\forall z\in My)$，これは $u\neq v\in I(M)$ ならば $My\cap C_G(v)=\phi$ を示す．したがって

$$|\mathscr{F}| = (|C_M(u)\backslash C_G(u)|-1)|I(M)|+1 = \left(\frac{2k}{n}-1\right)f+1$$

となり (i) が示された．$C_G(u)\simeq K$ の構造から，$My\cap C_G(u)=C_M(u)y$ はすべて位数 2 の元からなるか，あるいは位数 2 の元を一つも含まないから，$I(M)$ の各元 u に対して $My\cap C_G(u)\neq\phi$，$M\neq My$ なるすべての My の和集合に含まれる位数 2 の元の総数は k ($=C_G(u)-C_M(u)$ に含まれる位数 2 の元の数) であることがわかる．よって

$$\sum_{My\in\mathscr{F}}|My\cap I(G)| = k|I(M)|+|I(M)| = f(k+1).$$

すなわち (ii) が示された．$My\cap C_G(u)=\phi$ $(\forall u\in I(M))$ としよう．$F\ni z\neq 1$ とするとき $Myz\neq My$ である．実際，$Myz=My$ ならば，$1\neq z\in F\cap M^y$ となり (β) の (iii) に反する．したがって F は $M\backslash G-\mathscr{F}$ に半正則に作用し，$|F|\,|\,|M\backslash G|-|\mathscr{F}|$ を得る．これが (iii) である．最後に，(iv) を示すために $My\in M\backslash G-\mathscr{F}$，$My\cap I(G)\ni w$ とする．(β) の (iii) により $M\cap M^w\subseteqq C_M(v)$ $(\exists v\in I(M))$．よって $N_G(M\cap M^w)\ni w$ および $C_G(v)\simeq K\langle s\rangle$ の性質から，$M\cap M^w\neq 1$ ならば $w\in C_G(v)$．したがって $Mw=My\in\mathscr{F}$ となり矛盾である．よって $M\cap M^w=1$，とくに w により逆転される M の元は単位元に限る．これは，$|Mw\cap I(G)|=1$ を示す．▮

(ε) $M\backslash G=\mathscr{F}$ ならば $F=Q$，$D=K$ として定理 8.39 が成り立つ．

[証明] $M\backslash G=\mathscr{F}$ とすると

$$(2k+\varepsilon)(k+\varepsilon) = [G:C] = |I(G)| = f(k+1)$$

である．よって $\varepsilon=1$，$f=2k+1$ を得る．また

$$\frac{(2k+1)2k(k+1)}{nf} = [G:M] = \left(\frac{2k}{n}-1\right)(2k+1)+1$$

より，$n=k=|K|$．よって $N_G(F)=F\cdot K$．このとき，K は Frobenius 群 $N_G(F)$ の可換な Frobenius 補群であるから，定理 7.9 により巡回群である．したがっ

て (β) により $F=Q$, $D=K$ として定理が成り立つ. ▌

以下, $M\backslash G\neq\mathcal{F}$ と仮定する. このとき, (δ) の (i), (iii) により

$$|M\backslash G| \geqq \left(\frac{2k}{n}-1\right)f+1+f = \frac{2kf}{n}+1 \tag{8.101}$$

である.

(ζ) $f=k-1,\quad n=2,\quad \varepsilon=-1.$

[証明] (δ) の (i), (iv) により

$$\begin{aligned}[G:C] = |I(G)| &\leqq f(k+1)+|M\backslash G|-|\mathcal{F}| \\ &= f(k+1)+[G:M]-\left(\frac{2k}{n}-1\right)f-1,\end{aligned}$$

$$\therefore\quad [G:C]-[G:M] \leqq f(k+1)-\left(\frac{2k}{n}-1\right)f-1.$$

$|M|>|C|$ と仮定すると (8.101) により

$$\begin{aligned}\frac{2kf}{n}\left(\frac{nf}{2k}-1\right) &< [G:M](|M|/|C|-1) \\ &= [G:C]-[G:M] \\ &< f(k+1)-\left(\frac{2k}{n}-1\right)f-1,\end{aligned}$$

$$\therefore\quad k+2>f.$$

このとき, (γ) により $\varepsilon=-1$, $f\geqq k-1$, よって $f=k+1$ または $k-1$ であるが, $F\cap C=1$ より f は $[G:C]=(2k-1)(k-1)$ を割らねばならないから, $f=k-1$ である. また $n=|K\cap F|$ は $|K|=k$ と $|F|=k-2$ を割るから $n=2$. しかるにこのとき $2(k-1)=|M|>|C|=2k$ となり矛盾である. よって $nf=|M|\leqq|C|=2k$. このとき, (γ) により $\varepsilon=-1$, $f=k-1$, $n=2$ でなければならない. ▌

(η) $Y=G-C^G-F^G$, $Y\ni y$ とする.

(i) Y は G の二つの共役類からなり, y と y^{-1} がそれぞれの代表元である.

(ii) $|C_G(y)|=2k-1$. $2k-1$ は或る素数 p の巾である.

[証明] K, F は TI 集合であるから,

$$|C^G| = |K^G| = [G:C](k-1)+1 = (2k-1)(k-1)^2+1,$$

$$|F^G| = [G:N_G(F)](f-1)+1 = 2(k-1)(k-2)+1.$$

よって

(8.102) $$|Y| = |G|-|C^G|-|F^G|+1 = 4k(k-1)$$

である．また，K, F の TI 性と $|G|=|K||F|(2k-1)$ より $|C_G(y)|$ は $2k-1$ を割らなければならない．$(2k-1)/|C_G(y)|=m$ とおくと，

$$|y^G| = |G|/|C_G(y)| = 2k(k-1)m \qquad (m: \text{奇数})$$

である．よって $Y \supseteq y^G$ および (8.102) により $m=1$ でなければならない．すなわち $|C_G(y)|=2k-1$ で Y は G の二つの共役類からなる．$y^z=y^{-1}$ $(z \in G)$ とする．このとき，$z^2 \in C_G(y)$ であるが $C_G(y) \cap C^G=1$ より $z^2=1$．よって y を適当な共役でおきかえて $y^t=y^{-1}$ と仮定してよい．このとき，$\beta_I(y)=|C_G(y)|=2k-1 \geqq k+3$ であるから y は (γ) の (i), (ii) を満たし，したがって (ε), (δ) により $|C_G(y)|=2k+1$ または $k-1$ でなければならない．これは $|C_G(y)|=2k-1$ に反する．したがって y と y^{-1} は G で共役ではない．さて Y は G の二つの共役類からなるから，Y の元の位数は或る奇素数 p でなければならないが，$C_G(y)-\{1\} \subseteq Y$ であるから，$C_G(y)$ は p 群である．▌

(θ) p を (η) の (ii) における素数とする．G の Sylow p 部分群 Q は定理 8.39 の主張を満たす．

[証明] 最初に

(＊) G の Sylow p 部分群は TI 集合

であることを示そう．P_1, P_2 を G の異なる Sylow p 部分群として，$P_1 \cap P_2=H$, $N=N_G(H)$ とおく．$H \neq 1$ と仮定して矛盾を導こう．$P_1 \neq P_2$ より $N_{P_1}(H) \supsetneqq H$, $N_{P_2}(H) \supsetneqq H$. とくに $N_{P_1}(H) \neq N_{P_2}(H)$ であり N は少なくとも二つの Sylow p 部分群をもつ．r を N の位数を割る p と異なる任意の素数，$R \in \mathrm{Syl}_r(N)$ とする．$|G|=|F||K|p^c$ であるから，$r \mid |F|$ または $r \mid |K|$ である．$r \mid |K|$ ならば，R は K の或る共役 K^x に含まれるが K の TI 性から $N_N(R) \subseteq N_G(K^x)=C^x$ である．しかるに $[C : N_G(K)]=2$, $|N_N(R)|=$奇数であるから，$N_N(R) \subseteq K^x$ となり，$N_N(R)$ は Abel 群である．同様に $r \mid |F|$ のときも $N_N(R)$ は Abel 群である．このとき Burnside の定理 7.14 により N は r 巾零である．r は p と異なる任意の素数であるから，N の Sylow p 部分群は N の正規部分群となり (問 7.23)，これは N が少なくとも二つの Sylow p 部分群をもつことに反する．これで (＊) が示された．(＊) と補題 8.16 により

(＊＊) Q の 2 元が G で共役ならば $N_G(Q)$ で共役

である．$Z(Q)\ni y\neq 1$ とすると (η) の (i) により $Q-\{1\}$ の各元は y または y^{-1} と G で共役であるから $(**)$ により $Q=Z(Q)$，すなわち Q は Abel 群である．また，(η) の (ii) により Q は定理 8.39 の主張 (2) を満たす．このとき $N_G(Q)$ は Q を Frobenius 核とする Frobenius 補群である．$N_G(Q)=QD$，$Q\cap D=1$ としよう．このとき $(**)$ から $N_G(Q)$ の Q への共役による作用の軌道の長さは，1, $(q-1)/2$, $(q-1)/2$ $(q=|Q|)$ であるから，$|D|=(q-1)/2=|F|$．これは D と F が共役であることを示す．ところで，D は Frobenius 群 $N_G(Q)$ の可換な Frobenius 補群であるから，定理 7.9 により巡回群である．このとき定理 8.39 の主張 (3) は，(β), (ζ) から出る．▌

これで定理 8.39 の証明が完成された．

解答・ヒント

第1章

§1.1　**1.1**　$1^{-1}=1$, $(x^{-1})^{-1}=x$ は明らか．$(xy)(y^{-1}x^{-1})=(y^{-1}x^{-1})(xy)=1$ より $(xy)^{-1}=y^{-1}x^{-1}$.

1.2　$(x^{-1})^{-1}=x$ より全射であることが分かる．またこの式から，$x^{-1}=y^{-1}\Longrightarrow x=y$ も分かるから単射でもある．

1.3　$1x=x$ および $x^{-1}x=1\,(\forall x\in G)$ を示さねばならない．仮定により $x^{-1}x'=1$ なる x' が存在する．このとき $x^{-1}x=x^{-1}x1=x^{-1}xx^{-1}x'=x^{-1}x'=1$．また $1x=(xx^{-1})x=x(x^{-1}x)=x1=x$ である．

1.4　$H\ni x,y\Longrightarrow xy=(x^{-1})^{-1}y\in H$．$y=1$ として $x\in H$．よって部分群の条件(α)および(β)が成り立つ．

1.8　写像 $S\times T\ni(s,t)\to st\in ST$ が全射であることから，$|ST|\leqq|S||T|$．また写像 $T\ni t\to st\in sT$ は全単射であるから，$|T|=|sT|$．他も同様．

1.10　$x^{-1}Hx=x^{-1}H(x^{-1})^{-1}\subseteq H$．故に $xHx^{-1}\subseteq H$ と合わせて $xHx^{-1}=H$.

1.11　$N_G(S)\ni x$, $C_G(S)\ni y$, $S\ni s\Longrightarrow(xyx^{-1})s(xy^{-1}x^{-1})=xy(x^{-1}sx)y^{-1}x^{-1}=x(x^{-1}sx)x^{-1}=s$　$\therefore xC_G(S)x^{-1}\subseteq C_G(S)$

1.13　$H_iH_j\subseteq H_iH_iH_k=H_iH_k\subseteq(H_jH_k)H_k=H_jH_k\subseteq H_j(H_jH_i)=H_jH_i$．故に補題1.1により H_iH_j は部分群である．

§1.2　**1.15**　$(xH)^{-1}=Hx^{-1}$ に注意．

1.17　$x,y\in K$ のとき，$Hx=Hy\Leftrightarrow xy^{-1}\in H\cap K$．従って HK は H の右剰余類を $|K|/|H\cap K|$ 個含む．

1.18　$xSx^{-1}=ySy^{-1}\Leftrightarrow x^{-1}y\in N_G(S)$.

1.19　$x\equiv x', y\equiv y' \bmod n\Longrightarrow xy-x'y'=x(y-y')+y'(x-x')\equiv 0 \bmod n$．$(x,n)=1$ とすると例題1.2により $xx'+nn'=1$ なる $x',n'\in\boldsymbol{Z}$ が存在する．このとき $xx'\equiv 1 \bmod n$ である．

1.20　$N=\{x\in S\mid x\sim 1\}$ とおけ．

§1.3　**1.23**　指数関数：$\boldsymbol{R}\ni x\to a^x\,(a>0)$.

1.27　$g(xN)=f(x)N$ とおけばよい．ただし g のこの定義が well-defined であること，即ち $xN=yN\Longrightarrow f(x)N=f(y)N$ を言わねばならない．これを言うのに $N\subseteq\mathrm{Ker}(f)$ を用いる．

1.28　$(x,x,\cdots,x)\to(x_1N,x_2N,\cdots,xN_n)$ なる対応の核が $N_1\times N_2\times\cdots\times N_n$ である．

§1.4　1.32　ab の位数を k とすると $a^k=b^{-k}$. $a^{kn}=b^{-kn}=1$ より $m\mid kn$. $(m,n)=1$ だから $m\mid k$. 同様に $n\mid k$. よって $mn\mid k$. 一方明らかに $(ab)^{mn}=1$ すなわち $k\mid mn$. よって $k=mn$.

1.34　$\boldsymbol{C}^*$ の有限部分群 G の位数を n とすると，$G\ni\forall x$ に対して $x^n=1$. これは丁度 n 個の解を持つから，例題1.4より G は巡回群である.

1.35　$\boldsymbol{Z}_n$ を位数 n の巡回群と考え，生成元を a とする. $\mathrm{Aut}(\boldsymbol{Z}_n)\ni\sigma$, $\sigma(a)=a^k$ によって $\boldsymbol{Z}_n{}^*$ の元 k を定める. このとき，$\sigma\to k\in\boldsymbol{Z}_n{}^*$ なる対応が $\mathrm{Aut}(\boldsymbol{Z}_n)$ と $\boldsymbol{Z}_n{}^*$ の同型対応を与える.

§1.5　1.37　ヒントにより，$i<j$ のとき $(ij)=(i+1\,j)(i\,i+1)(i+1\ j)$. これをくり返す.

1.38　$SL_n(\boldsymbol{C})\ni A$ とする. A の左右から $R(i,j,c)$ の形の元を掛けて対角行列とすることができる(ヒントを参照). 従って2次行列 $\begin{bmatrix}c & 0\\ 0 & c^{-1}\end{bmatrix}$ が $R(i,j,c)$ の形の2次行列の積として書けることを示せばよい. 実際

$$\begin{bmatrix}c & 0\\ 0 & c^{-1}\end{bmatrix}=\begin{bmatrix}1 & 0\\ 1-c & 1\end{bmatrix}\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & c^{-1}\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ c(c-1) & 1\end{bmatrix}$$

1.42　Q_{4m} の元は a^i または a^ib で $(a^ib)^2=a^2$. これから $\langle a^m\rangle$ が Q_{4m} のただ一つの位数2の部分群であることが分かる.

1.43　Q_8 は位数8であるから，位数4の部分群はすべて正規. 位数2の部分群はただ一つであるから正規.

1.44　N の生成元を a, G/N の生成元を bN とする. a, bN の位数をそれぞれ m,n とすると，$a^m=1, b^n=a^k, b^{-1}ab=a^r$ なる k,r が存在する. このとき

$a^k=b^n=b^{-1}b^nb=b^{-1}a^kb=a^{rk}$ より $k\equiv rk \bmod m$, $a=b^{-n}ab^n=a^{r^n}$ より $r^n\equiv 1 \bmod m$.

$$\therefore G\cong \boldsymbol{Z}(m,n,r,k).$$

1.45　$T=\{(1),\ (1\ 2)\}$ とすると，$TST^{-1}\cap\mathfrak{A}_n=\{(1\ 2\ 3), (1\ 3\ 2), (1\ 2)(3\ 4), \cdots, (1\ 2)(n, n-1)\}$ である.

§1.6　1.46　n が奇数のときは，$O(n)\cdots SO(n)\ni -E_n$ である. よって $X\in O(n)-SO(n)$ ならば $X^{-1}AX=(-X)^{-1}A(-X)$, $-X\in SO(n)$.

1.48　$1^{a_1}2^{a_2}\cdots n^{a_n}$ 型の異なる元の数を数えればよい.

1.49　D_{2n} の類等式：

n が偶数のとき：$2n=1+1+2+\cdots+2+n/2+n/2$ (2は $(n-2)/2$ 個現れる)

n が奇数のとき：$2n=1+2+\cdots+2+n$ (2は $(n-1)/2$ 個現れる)

Q_{4m} の類等式：$4m=1+1+2+\cdots+2+m+m$ (2は $(m-2)$ 個現れる).

1.50　$\mathfrak{A}_4$ の類等式：$12=1+3+4+4$.

$\mathfrak{A}_5$ の類等式：$60=1+20+15+12+12$.

1, 20, 15, 12, 12 のいくつかの(1 を含む)和から 60 の約数を作るには 1 のみをとるか全体をとるしかない．これは問題の前半により $\mathfrak{A}_5$ の正規部分群が $\{1\}$ または $\mathfrak{A}_5$ 自身に限ることを示す．

§1.7　1.53　$a^2+b^2+c^2+d^2=1$ のとき，$a+bi+cj+dk$ に対応する行列は，行列式 1 の 2 次ユニタリー行列である．

1.54　例題 1.1 の証明を参照．

1.55　両側イデアル $I\neq M_n(k)$, $\{0\}$ をとる．$I\ni A\neq 0$ の (i,j) 成分 $a_{ij}\neq 0$ とすると行列単位 E_{ii}, E_{jj} を左右から掛けて $I\ni E_{ij}$ としてよい．このとき I は任意の行列単位 E_{kl} を含む．

1.58　ガウスの整数環 $\boldsymbol{Z}[i]$ $(i=-1)$ の乗法群は $\{\pm 1, \pm i\}$，$H_{\boldsymbol{Z}}$ の乗法群は $\{\pm 1, \pm i, \pm j, \pm k\}$

1.60　$\boldsymbol{Z}_m$ の直積分解については例題 1.5 を参照．

1.62　補題 1.7 を用いて，例題 1.1 と同じようにやる．

第2章

§2.1　2.1　(I, III $\Longrightarrow$ II)．III において $g=g'=1$ とおいて $1\circ x=1\circ(1\circ x)$．写像 $x\to 1\circ x$ は全射だから $1\circ y=y\ (\forall y\in\Omega)$．(II, III $\Longrightarrow$ I)．III において $g'=g^{-1}$ とおけ．

2.4　V に底を定めて数ベクトル空間 k^n として表わし

$$\begin{bmatrix} x & 0 \\ y & x^{-1} \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=\begin{pmatrix} x \\ y \end{pmatrix},\quad \begin{bmatrix} 0 & x^{-1} \\ x & 0 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=\begin{pmatrix} 0 \\ x \end{pmatrix}(k\ni x\neq 0)\text{ を用いる．}$$

2.5　$O(n)$ が可移であること：任意の $\boldsymbol{a}=(a_1, a_2, \cdots, a_n)\in S^{n-1}$ に対して，$\boldsymbol{e}_1=(1, 0, \cdots, 0)$ を $\boldsymbol{a}$ に移す $A\in O(n)$ が存在することを言えばよい．それには，$\boldsymbol{R}^n$ の正規直交基底に $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n$ $(\boldsymbol{a}=\boldsymbol{a}_1)$ をとり，これらのベクトルを行とする n 次行列を A とすればよい．

$SO(n)$ が可移であること：ベクトル $(a_1, a_2, \cdots, a_n)$ を固定する．このベクトルを $(-a_1, a_2, \cdots, a_n)$ に移す $SO(n)$ の元があればよい．これは $n=2$ のとき見ればよいが，それは幾何学的に明らか．

2.7　$x, y\in X$, $n\circ x=y$ $(n\in N)$ のとき，$N\ni n'=gng^{-1}$ で $n'\circ(g\circ x)=gn\circ x=g\circ y$．

§2.2　2.9　定理 2.1 系により (G, Ω) の各軌道の元の数は p のベキであるから，Ω の元の数が p と素のときは，長さ 1 の軌道がなければならない．

2.10　p 群 G の $N-\{1\}$ への作用 $n\to gng^{-1}$ を考えると，補題 2.1 により固定点がある．これは $N\cap Z(G)\neq 1$ を示す．

2.11　例題 2.2 参照．

2.12　位数 p^3 の非アーベル群：

$$a^{p^2}=1,\qquad b^p=1,\qquad b^{-1}ab=a^{p+1}$$

位数 pq の非アーベル群：$p\equiv 1 \bmod q$ のとき，$r^q\equiv 1 \bmod p$ なる r が存在する．このとき，$a^p=1, b^q=1, b^{-1}ab=a^r$.

2.13 $q\equiv 1 \bmod 4$ のとき．$a=\begin{bmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{bmatrix}$，（$\alpha$ は $\boldsymbol{F}_q{}^*$ の乗法群の生成元），$b=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}$ とすると，a, b は，位数 $2(q-1)$ の4元数型の群を生成し，$SL(2, q)$ の 2-シロー群を含む．$q\equiv -1 \bmod 4$ のときは，$SL(2, q^2)$ で考えよ．$PSL(2, q)$ については，問 1.42 参照．

§2.4 2.14 $SL(2,2)$ は位数6だから位数3の部分群は正規部分群である．

$SL(2,3)$：

$$a=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\ b=\begin{bmatrix}1 & -1\\ -1 & -1\end{bmatrix},\ c=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

とする．a, b は位数8の4元数群を生成し，$c^{-1}\langle a, b\rangle c=\langle a, b\rangle$ である．$SL(2,3)$ の位数は24であるから a, b, c は $SL(2,3)$ の生成元で $\langle a, b\rangle$ は $SL(2,3)$ の正規部分群である．

2.15 $[O(2):SO(2)]=2, SO(2)$ は可換群である．

2.16 $SU(n)$ の共役類の代表元として対角行列がとれる．あとは例題 2.4 と同じ．

§2.6 2.17 $\Omega\ni x$ の固定部分群を $H, \Omega\ni y$，$gxg^{-1}=y$ とすると，y の固定部分群は $gHg^{-1}=H$ である．従って H は Ω の各点を固定する．このとき，(G,Ω) の忠実性により $H=1$.

2.18 補題 2.4 により，(N,Ω) は可移である．

2.19 $\Omega\ni b\neq a$ とすると，$n\circ a=b$ なる $N\ni n\neq 1$ がただ一つ存在する．このとき，$b\to n$ なる対応が，同型 $(G_a, \Omega-\{a\})\cong(G_a, N^\sharp)$ を与える．

第3章

§3.1 3.1 $(k+1)$ 次小行列式をある列または行で展開してみればよい．

3.2 問 1.38 を参照．

§3.2 3.4 $\boldsymbol{a}=(a_1, a_2, \cdots, a_n)$ とおく．(i) $\Longrightarrow$ (ii). $\boldsymbol{a}$ で生成される $\boldsymbol{Z}^n$ の部分加群に定理 3.3 を適用せよ．(ii) $\Longrightarrow$ (iii). $\boldsymbol{a}$ を含む $\boldsymbol{Z}^n$ の基底を $\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n$，$\boldsymbol{a}_i=\sum a_{ij}\boldsymbol{e}_j$，$A=(a_{ij})\in M_n(\boldsymbol{Z})$ とすると，行列 A の第一行は $\boldsymbol{a}$ であり，また補題 3.2 により $\det(A)=\pm 1$ である．(iii) $\Longrightarrow$ (i). 明らか．

§3.4 3.7 (3.9) は明らか．後半は例題 1.5，定理 1.6 の証明参照．

第4章

§4.1 4.1 可換群が単純群であるためには，素数位数であることが必要十分である．

§4.2 4.6 (i) $\Longrightarrow$ (ii). 条件 (γ) による．(ii) $\Longrightarrow$ (iii). 明らか．(iii) $\Longrightarrow$ (i). (γ) を示せばよい．$i\neq j$ ならば $G_i\cap G_j=1$，よって G_i の元と G_j の元は交換可能．$x_1x_2\cdots x_n=y_1y_2$

$\cdots y_n$ $(x_i, y_i \in G_i)$ ならば $x_1^{-1}y_1 = x_2^{-1}y_2 \cdots x_n^{-1}y_n$，よって(iii)により $x_1 = y_1$ かつ $x_2 \cdots x_n = y_2 \cdots y_n$．以下同様に続けて $x_i = y_i$ $(i=2, 3, \cdots, n)$．

4.7　$\boldsymbol{Z}$ の部分群 $H_1, H_2 (\neq 1)$ を任意にとると $H_1 \cap H_2 \neq 1$ である．$G(p)$, $\boldsymbol{Q}$ についても同様．

第5章

§5.1　**5.2**　(i)　$x \in L, h \in H, k \in K$ とする．$x^{-1}h^{-1}xh \in K \subseteq H$ より $x^{-1}hx \in H$，すなわち $x \in N_G(H)$．$x^{-1}k^{-1}xk \in K$ より $x \in N_G(K)$．(ii) $x, y \in L \Longrightarrow [xy, h] = [x, h]^y[y, h]$．(i)により $[x, h]^y \in K$ だから $xy \in L$

5.3　問5.2から出る．

§5.2　**5.5**　$x \in G$ とすると，$H \ni h \to x^{-1}hx$ なる対応は H の自己同型で K は H の特性部分群であるから $x^{-1}Kx = K$.

5.7　(i)　$D(G)$ が G の中心に含まれることに注意して(5.4)を用いる．(ii)　n に関する帰納法．

$$\begin{aligned}(xy)^{n+1} &= x^n y^n [y, x]^{n(n-1)/2} xy = x^n y^n xy [y, x]^{n(n-1)/2} \\ &= x^{n+1} y^{n+1} y^{-1} (y^{-n} x^{-1} y^n x) y [y, x]^{n(n-1)/2} \\ &= x^{n+1} y^{n+1} [y^n, x][y, x]^{n(n+1)/2} \\ &= x^{n+1} y^{n+1} [y, x]^n [y, x]^{n(n-1)/2} \\ &= x^{n+1} y^{n+1} [y, x]^{n(n+1)/2}\end{aligned}$$

5.8　行列の計算．

5.9　$\mathfrak{A}_3 = K_1(\mathfrak{S}_3) = K_2(\mathfrak{S}_3) = \cdots$，$\mathfrak{A}_4 = K(\mathfrak{S}_4) = K(\mathfrak{S}_4) = \cdots$ であることを確かめよ．

5.10　必ずしも成立しない．

5.13　直接の計算．

5.14　定理5.3, (i)による．

§5.3　**5.15**　$1 = [H, K, K] = [K, H, K]$ であるから，3部分群補題により $[K, K, H] = 1$，すなわち $[K', H] = [H, K'] = 1$. (5.21)も同様．

第6章

§6.3　**6.1**　$a_n \to 1/n!$ $(n=1, 2, \cdots)$ なる対応により $\langle a_1, a_2, \cdots \rangle$ から Q(有理数体の加法群)の上への準同型が得られる．この写像が同型を与えることを見るには

$$k_1/1! + k_2/2! + \cdots + k_n/n! = 0 \quad (|k_i| < i)$$
$$\Longrightarrow k_1 = k_2 = \cdots = k_n = 0$$

を見ればよい．

6.2　(i)は直接の計算で分かる．(ii)については例6.5を参照．

6.3 $SL(2,Z)$ から $PSL(2,p)$ への自然な準同型を考え，例 6.5 を参照せよ．

第7章

§7.1 7.1 $P \in \mathrm{Syl}_p(\Phi(G))$ に対して補題 7.1(ii)，補題 7.2 により $G=N_G(P)\Phi(G)=\langle N_G(P), \Phi(G)\rangle=N_G(P)$．よって $G \triangleright P$，とくに $\Phi(G)\triangleright P$．これは $\Phi(G)$ がベキ零群であることを示す．

7.2 $(p,p,\cdots,p)$ 型の群の極大部分群は，指数 p の部分群に他ならない．よって任意の元 $(\neq 1)$ に対してそれを含まない指数 p の部分群の存在を示せばよい．

7.3 補題 7.5 の証明と同様．

7.6 $n \geqq 4$ のとき，置換 $(1\ 2), (1\ 2)(3\ 4)(5\ 6)$ で生成される位数 2 の部分群 $\langle(1\ 2)\rangle$，$\langle(1\ 2)(3\ 4)(5\ 6)\rangle$ は共に $\mathfrak{S}_n/\mathfrak{A}_n$ の補群である．

7.7 $\mathfrak{S}_4/\mathfrak{A}_4$ の任意の補群は $\{1,2,3,4\}$ のうちの 3 文字 $\{i,j,k\}$ の上の対称群である．

§7.2 7.8(p. 165) 定理 7.4 の応用．

7.9 $C_X(A) \ni yz\ (y \in Y,\ z \in Z,\ a \in A) \Longrightarrow yz=(yz)^a=y^a z^a \Longrightarrow z^a z^{-1}=y^{-a}y \in Y \cap Z$．定理 7.5 の X, Y として $Z, Y\cap Z$ をとると，$z=hz'\,(h \in Y\cap Z, z' \in C_Z(A))$．よって $yz=yhz'=y'z'\,(y' \in Y, z' \in C_Z(A))$．このとき，$y' \in C_Y(A)$．

7.10 (i) X の A 不変極小部分群を Y とすると，定理 7.6(i) により Y は p 群，Y の中心 $Z(Y)\,(\neq 1)$ を考えるとこれは A 不変だから Y は Abel 群，Y の位数 p の元および単位元からなる Y の部分集合は A 不変部分群．よって Y は基本 Abel 群である．(ii) X は A 不変極小部分群である．

7.11 ヒントに従え．

7.14 ヒントに従え．

7.15 H を $\Omega \ni a$ の固定部分群とすると，$H\cap H^x$ は a および a^x を固定する．(β) により $a=a^x$ すなわち $x \in H$．逆に G, H が (7.26) をみたすとする．$xH=H, xyH=yH\ (y \notin H)$ とすると $x \in H, y^{-1}xy \in H \cap H^y$．(7.26) により $y^{-1}xy=1$．よって $x=1$．すなわち (β) が成り立つ．

7.17 ヒントに従え．

7.18 (i) $SL(2,p)$ の位数は $p(p-1)(p+1)$ で位数 $p-1, p+1$ の巡回部分群を持つ．(位数 $p+1$ の元の存在に関しては，定理 8.33 を参照)．これから (i) が分かる．(ii) $SL(2,p)$ の位数 2 の元は $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ に限ることを示し，補題 7.20 を用いよ．

§7.3 7.24 問 7.23 を用いよ．

7.25 $G=\mathfrak{S}_4$ (4 次対称群)，$P \in \mathrm{Syl}_2(G)$ とすると，$J(P)=P, C(Z(P))=P$．よって G は定理 7.15 の仮定をみたす．しかし 4 次対称群は 2 ベキ零ではない．

7.26 ヒントに従え.

§7.4 7.30 ヒントに従え.

7.31 $G \triangleright N$ とする. $O_{p'}(N)=1$ としてよい. $E(N) \subseteq E(G)=1$ だから $F^*(N)$ は p 群. よって N は p 束縛である.

7.32 (i), (ii) はそれぞれ $O_{p'}(N_G(H)) \subseteq C_G(H)$, $E(N_G(H)) \subseteq C_G(H)$ に注意. (iii) は問 7.31 から出る.

7.34 Jordan の標準形を考えよ.

7.35 問 7.32(iii) と補題 7.29 を用いよ.

7.36 行列の計算をして確かめよ.

7.37 ヒントに従え.

第8章

§8.1 8.2 $(1\ 2) \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, $(1\ 2\ 3) \longrightarrow \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

8.4 $v_1, v_2, \cdots, v_n$ を (G の置換表現の) 表現空間の底とするとき, ベクトル $v=v_1+v_2+\cdots+v_n$ は G 不変である.

§8.2 8.7 $G=\{g_1, g_2, \cdots, g_n\}$ とするとき, $f_i(g_j)=\delta_{ij}$ によって $f_i \in k(G)$ を定めると, $\langle f_i \rangle \cong k$, $k(G) \cong k+k+\cdots+k$ である.

8.8 ヒントに従え.

§8.3 8.9 p. 248 の (8.7) を参照.

8.10 4 個の 1 次表現のほかに, 例 8.4(p. 245) の記号を用いて $Q_1, Q_2, \cdots, Q_{n-1}$ なる $n-1$ 個の 2 次表現が既約表現である.

8.11 4 次交代群 $\mathfrak{A}_4$ の交換子群は $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ なる位数 4 の部分群であるから, 直ちに 3 個の 1 次表現が得られる. また共役類の数は 3 であるからもう一つの既約指標は直交関係から得られる.

8.12-8.13 ヒントに従え.

8.14 (i) φ に対する等式 (8.36) の両辺に $\psi(b^{-1})$ を掛け, b を G の共役類の代表系を走らせて辺々加えると,

$$g\varphi(a)(\varphi, \psi) = \varphi(1)(\varphi * \psi)(a) \qquad (g=|G|)$$

を得る. ここで $\varphi * \psi$ は §8.2 の注意 1 (p. 257) で定義されている群環 $\boldsymbol{C}(G)$ の積である. φ と ψ の役割を入れ換えて $g\psi(a)(\psi, \varphi)=\psi(1)(\psi * \varphi)(a)$ であるが, $\varphi, \psi \in \boldsymbol{C}(G)$ のとき, $\varphi * \psi = \psi * \varphi$ である. (ii) $(\chi, \psi) \neq 0$ なる既約指標 ψ をとり, χ, ψ に対して (i) を用いると, $\chi(a)=c\psi(a)$ $(c=\chi(1)/\psi(1))$ が任意の $a \in G$ に対して成り立つが, $(\chi, \chi)=(\psi, \psi)=1$ より

$c=1$，従って $\chi=\psi$ を得る．

§8.4 **8.15** ヒントに従え．

8.17 (ii) Z を超可解群 G の中心で $G\neq Z$ とする．$\bar{G}=G/Z$ は(i)により超可解群だから，$\bar{G}=\bar{G}_0\supseteq\bar{G}_1\supseteq\cdots\supseteq\bar{G}_{n-1}\supseteq\bar{G}_n=1$，$\bar{G}\triangleright\bar{G}_i$, $\bar{G}_{i-1}/\bar{G}_i$ は巡回群なる列をとると，G_{n-1}(=$\bar{G}_{n-1}$ の逆像)は可換正規部分群である．(iii) 定理 8.21 の証明を参照．

8.18 4 次対称群 $\mathfrak{S}_4$ の指標表は例 8.11 (p. 276) を参照．$\mathfrak{S}_4$ の指数 3 の部分群 $\langle(1\ 2\ 3\ 4), (2\ 4)\rangle$ は位数 8 の正 2 面体群である．この群の適当な 1 次指標を誘導すると $\mathfrak{S}_4$ の二つの 3 次既約指標が得られる．また 4 次交代群の自明でない 1 次指標を誘導して 2 次既約指標を得る．

8.19 $SL(2,3)$ は指数 2 の部分群を持たないことを示せ．

§8.6 **8.23** 一般に χ を群 G の指標とするとき，$\sum\chi(x)$ (x は G の全ての元を走る)は G の位数で割れること(直交関係！)に注意．

8.25 ヒントに従え．

§8.7 **8.26** 単射であることは，補題 8.17 の(i)による．$\psi\in M_G(D^G)$ とするとき，$\psi\mid H=\varphi$ とおくと，条件 $D^x\cap N_G(D)\subseteq D\,(\forall x\in G)$ により $\varphi\in M_H(D), \varphi^G=\psi$ である．

8.27 ヒントに従え．

§8.8 **8.29** (i) G の位数は p^{2n+1} で交換子群 G' は対角線成分が 1，それ以外の成分は $(n+2, n+2)$ 成分を除いて 0 であるような行列からなる位数 p の部分群である．またこの部分群 G' は G の中心とも一致する．このことから G の共役類は G' の各元からなる p 個，G' の各剰余類($\neq G'$)からなる $p^{2n}-1$ 個，計 $p^{2n}+p-1$ 個からなることが分かる．従って G は 1 次指標を p^{2n} 個持つが，その他の $p-1$ 個の既約指標の次数を $x_1, x_2, \cdots, x_{p-1}$ とすると直交関係より

$$p^{2n}+{x_1}^2+{x_2}^2+\cdots+{x_{p-1}}^2=p^{2n+1}$$

一方 G は位数 p^{n+1} の可換部分群をもつから Frobenius 相互律により $x_i\leqq p^n$．従って $x_1=x_2=\cdots=x_{p-1}=p^n$ を得る．(ii) 次数 p^n の既約指標は直交関係により $G-G'$ の上で値 0 を取ることに注意せよ．

あ と が き

群の一般論を解説した書物は，和文欧文を問わず数多く出版されている．本書の第1-6章と第8章の前半(§8.1-§8.4)で解説したことは，それらの書物でも必ず取り扱われている事柄であり，記述も類型化されているといってもよい．本講の記述もその類型をでるものではない．いま振り返ってみて，いくつかの点で意に満たぬ点も無いではないが，ただただ読者の御批判を待つのみである．第7章と第8章の後半では，近年の有限群論からいくつかの題材を選んで解説した．そこでは，Glauberman, Bender などの最近の論文をいくつか利用した．とくに§7.4, d)で述べた2信号関手定理の Bender による証明は，本書執筆時には未発表であったものを利用させて頂いた．また§8.8, a)で述べた Brauer-Fowler の定理8.36-8.37の証明は，§8.6, a)で引用した M. Isaacs: Character Theory of Finite Groups, Academic Press (1976) によるものである．

筑波大学の八牧宏美氏は，本書の原稿7章までを精読され多くの有益な助言を与えられた．ここに記して感謝したい．

欧 文 索 引

和 文 索 引

ア 行

カ 行

サ 行

群　論　　　　　　　　　　　　　　岩波基礎数学選書

1991年1月10日　第1刷発行 ©
2011年6月24日　第3刷発行

著　者　近藤　武（こんどう　たけし）

発行者　山口昭男

発行所　株式会社 岩波書店
〒101-8002 東京都千代田区一ツ橋 2-5-5
電話案内 03-5210-4000
http://www.iwanami.co.jp/

印刷・精興社　製本・三水舎

ISBN 4-00-007807-0　　　Printed in Japan